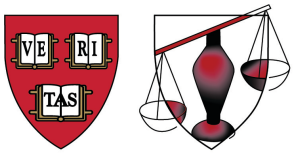


Berkman

The Berkman Center for Internet & Society
at Harvard University

Research Publication No. 2015-5
February 18, 2015

Governance of Online Intermediaries
Observations From a Series of National Case Studies

Urs Gasser
Wolfgang Schulz

23 Everett Street • Second Floor • Cambridge, Massachusetts 02138
+1 617.495.7547 • +1 617.495.7641 (fax) • http://cyber.law.harvard.edu •
cyber@law.harvard.edu

Urs Gasser and Wolfgang Schulz

GOVERNANCE OF ONLINE INTERMEDIARIES: OBSERVATIONS FROM A SERIES OF NATIONAL CASE STUDIES

February 18, 2015
The Berkman Center for Internet & Society Research Publication Series

WITHIN THE

GLOBAL NETWORK OF **INTERNET AND SOCIETY** RESEARCH CENTERS

ACKNOWLEDGEMENTS

This synthesis and case study series would not have been possible without the dedication and hard work of many contributors from the Network of Centers (NoC) and the Berkman Center. In particular, we would like to thank our case study authors, who dedicated countless hours to this project and whose efforts were instrumental in its completion. Many thanks also to our friends and collaborators Raimondo Iemma, Felix Krupar, Juan Carlos De Martin, Mayte Peters Schomburg, Dana Walters, and Jonathan Zittrain for guidance, collaboration, and support.

We wish to extend our gratitude to Adam Holland and Andy Sellars for conceptual guidance and editorial work, and Gretchen Weber for communications support. Special thanks are due to Annie Pruitt for coordinating this research effort and providing extensive editorial support.

The Berkman Center is grateful for workshop support by the Radcliffe Institute for Advanced Studies, and grant support by the MacArthur Foundation.

Urs Gasser

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

Urs Gasser & Wolfgang Schulz[1]

[1]Urs Gasser serves as Executive Director of the Berkman Center for Internet & Society at Harvard University and Professor of Practice at Harvard Law School. Wolfgang Schulz is Director of the Hans-Bredow Institute and the Humboldt Institute for Internet and Society, and Professor of Law at the University of Hamburg. The authors wish to thank Annie Pruitt for editorial assistance and the contributors to the Network of Center's Online Intermediaries project for their collaboration, and the MacArthur Foundation for providing seed funding to the Berkman Center for this research initiative. For additional information on the initiative, please contact Urs Gasser, Berkman Center for Internet & Society, at ugasser@cyber.law.harvard.edu

Table of Contents

I. Introduction

Online intermediaries in various forms – including search engines, social media, or app platforms – play a constitutive role in today's digital environment. They have become a new type of powerful institution in the 21st century that shape the public networked sphere, and are subject to intense and often controversial policy debates. This paper focuses on one particular force shaping the emergence and future evolution of online intermediaries: the rapidly changing landscape of *intermediary governance* at the intersection of law, technology, norms, and markets. Building upon eight in-depth case studies and use cases, respectively, this paper seeks to distill key observations and provide a high-level analysis of some of the structural elements that characterize varying governance regimes, with a focus on intermediary liability regimes and their evolution.

Analyzing online intermediary governance issues from multiple perspectives, and in the context of different cultures and regulatory frameworks, immediately creates basic problems of semantic interoperability. Lacking a universally agreed-upon definition,[2] this synthesis paper and its' underlying case studies are based on a broad and phenomenon-oriented notion of online intermediaries, as further described below. In methodological terms, the observations shared in this synthesis paper offer a selective reading and interpretation by the authors of the broader take-ways of a diverse set of case studies examining online intermediary governance frameworks and issues in Brazil, the European Union, India, South Korea, the United States, Thailand, Turkey, and Vietnam.[3] These case studies, in turn, have emerged in the context of an international research pilot by the Global Network of Internet & Society Research Centers (NoC), through a process of in-person consultations and remote collaborations among the researchers, and are based on a set of broader questions regarding the role of online intermediaries in the digital age.[4]

As a synthesis document, this paper is not aimed at providing a detailed or even comprehensive discussion of online intermediary governance, but it is rather intended to capture some of the insights and observations emerging from the analysis and comparative discussion of a limited – albeit diverse – sample of national regimes through an internationally coordinated academic research effort. The synthesis paper therefore does not cover all aspects of intermediary governance, but focuses on the issues that are examined in the case studies.

For a more detailed account of country-specific frameworks and their interaction with online intermediaries, as well as a deeper analysis of the issues highlighted in this paper, we refer to the set of case studies released in tandem with this synthesis. Together, these materials seek to complement important policy-oriented research efforts on online intermediaries by strengthening

[2] But see OECD. *The Economic and Social Role of Online intermediaries* (2010), 9. http://www.oecd.org/Internet/ieconomy/44949023.pdf: "'Online intermediaries' bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties."

[3] See Appendices A – H for the full text of the case studies. Additionally, the case studies are available for comment at https://publixphere.net/i/noc/page/Online_Intermediaries_Research_Project_Case_Studies.

[4] The process is documented at: "Online Intermediaries: Functions, Values, and Governance Options", The Global Network of Internet & Society Research Centers, 2014 https://drive.google.com/file/d/0B_ToTBKP5ITVWTl0UzV0U3B2RlU/view?usp=sharing.

the evidence-base,[5] and contributing to our shared understanding of the various policy options available, including their impact on, and interplay with, online intermediaries.

II. Terminologies and Perspectives

A. Framework

Recently, there has been an exponential increase in the use of the ambiguous term "intermediaries" in policy debates, which corresponds with the emergence of a new category of actor in the digitally networked environment and suggests a structural – and not just incremental – change in the information ecosystem.

Despite a number of important studies in this area,[6] the phenomenon is still a moving target and the term "intermediary" often serves as a fallback phrase in the absence of a clear-cut definition. In certain policy contexts and jurisdictions, the term is sometimes used as a rhetorical tool to indicate that a given service does not fall within the category of traditional media services and – consequently – is not encompassed by traditional media regulation. These issues of qualification and categorization under existing laws and policies are another reason why the meaning of the term should be carefully reflected upon.

Various disciplines conduct research on online intermediaries and are likely to frame this research differently, as an initial literature review in the context of this project suggests.[7] But different approaches to the phenomenon also exist within individual domains or disciplines. From a legal perspective, for instance, there are various angles from which to look at the

[5] See in particular the efforts by the United Nationals Organization for Education, Science and Culture (UNESCO) (e.g. UNESCO, The Open Society Foundation, and the Internet Society, "The Freedom of Expression Online – The Role of Online intermediaries". Executive Summary. [Presented at IGF, Istanbul, September 5, 2014]http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/foe_online_intermediaries.pdf); the World Intellectual Property Organization (WIPO) (e.g. "Online intermediaries and Creative Content." World Intellectual Property Organization. http://www.wipo.int/copyright/en/Internet_intermediaries/); La Rue, Frank. "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression." 2013. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf; generally, the United Nations Department of Economic and Social Affairs (UNDESA), the Center for Democracy and Technology (CDT) (e.g. "Intermediary Liability | Center for Democracy & Technology." https://cdt.org/issue/free-expression/intermediary-liability/.); the Association for progressive Communication (APC) (e.g. "Intermediary Liability." The Association for Progressive Communication. January 1, 2014. https://www.apc.org/en/irhr/intermediary-liability.), "Online intermediaries: Dilemma of Liability." Article 19. Accessed December 10, 2014. http://www.article19.org/resources.php/resource/37242/en/Internet-intermediaries:-dilemma-of-liability., "Intermediary Liability | Center for Democracy & Technology." Accessed December 10, 2014. https://cdt.org/issue/free-expression/intermediary-liability/.; *and* "The Manila Principles On Intermediary Liability: Version 0.9," Organization, December 1, 2014, https://docs.google.com/document/d/1kAkqgt3cRb65d8ik6vWYgpk6DYpP8ABA43ljgDiGOf8/edit?usp=sharing.

[6] Most notably the work of the OECD, see in particular OECD. *The Economic and Social Role of Online intermediaries*. 2010. p. 9. http://www.oecd.org/Internet/ieconomy/44949023.pdf and the other efforts mentioned supra, note 4. See also, "Fostering Freedom Online – The Role of Online intermediaries," United Nations Organization for Education, Science, and Culture (UNESCO). 19 Jan. 2015. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

[7] Kulk, Stefan, Tijana Milosevic, and Melinda Sebastian. "Online Intermediaries: A Thematic Analysis of their Social Role and Functions," The Global Network of Internet & Society Center, Working Paper, 2014. https://docs.google.com/document/d/1h1WmsijKVWgrky2GHhqqI1lytZejkwnMc35CZKeeUXU/edit?usp=sharing.

phenomenon, which might lead to different definitions. In countries that have enacted a specific framework for media regulation, the main difference might be the service's impact on public opinion making. In regards to *liability*, the focus might lie in the control over and the technical ability to take content down. From the perspective of *freedom of speech*, intermediaries perform a new type of activity and create a space for individuals to express themselves online, a function that can be examined in greater depth.

Economists are interested in the location of online intermediary services within the value chain. It is characteristic that intermediaries are positioned between content providers and customers. Furthermore, the added value that intermediaries create might help to frame this group of services. From a *media studies* perspective, the way that services are integrated into daily life and the meaning that we collectively create by using intermediaries – e.g. the creation of new types of public spheres – is important. Intermediaries are associated with specific social practices and these practices, in turn, reflexively construct the service provided. In a similar fashion, studies on technical artifacts as institutions can ask how entities like algorithms, on which many online intermediary services are based, can be seen as institutions.

In the context of this cross-jurisdictional and cross-disciplinary research effort, we do not attempt to come up with a uniform definition of online intermediaries. Rather, we take a phenomenological approach and use socially and economically significant real world services as guiding examples. As such, this research effort has focused on services that are: (a) "in between" content and users; (b) show structural relevance to public communication (i.e. are not merely private); and (c) are not traditional journalistic-editorial ("media") services. We are aware that the various elements of this definition refer to complex concepts, however, the definition serves as a workable proxy for the purposes of the case studies.

Core examples of "online intermediaries" that surfaced within this framework and were examined in the context of the case studies include search engines, micro blogs, social media, and user generated content platforms, among others. The intention of this research effort is not to limit the study of this subject to those cases, but use them *pars pro toto* to distill the essential characteristics of online intermediaries.

B. Observations

With this tentative framework in mind, the analysis of the case studies leads to a series of high-level observations regarding questions of definition, categorization, and typology. At a basic level, the legal frameworks we reviewed revealed a significant variety in the definitions of online intermediaries.[8] In some jurisdictions, platforms that might be seen as "edge cases" under the parameters outlined above are defined as intermediaries and have been examined in the respective country cases study. The IT Act of India, for instance, sets forth a very broad definition of intermediaries, including telecommunication carriers, Internet service providers, and other backbone services.[9] In the Turkish case study, to take a second example, e-commerce

[8] See also "The Manila Principles On Intermediary Liability: Version 0.9," December 1, 2014. https://docs.google.com/document/d/1kAkqgt3cRb65d8ik6vWYgpk6DYpP8ABA43ljgDiGOf8/edit?usp=sharing.
[9] Arun, Chinmayi, and Sarvjeet Singh. "Online Intermediaries Case Studies Series: Online Intermediaries in India", The Global Network of Internet & Society Research Centers (2015), 8.

platforms have played a key role in conflicts over intermediary liability and thus serve as an important use case in this research effort.[10]

The type of intermediary that plays a key role in a given policy or legal debate is context-specific and depends on various factors, particularly the country or region's political economy. In the European Union, search engines such as Google have largely dominated legal and policy conversations. The most visible manifestation of this situation can be seen in the recent CJEU ruling on the so-called "right to be forgotten" or, more precisely, the "right to be delisted".[11] While the former could be construed to mean the right of an affected person to have certain information completely wiped from the Internet, the "right to be delisted" constitutes the right to have information deleted from the listings of search engines and web catalogues, thus merely erasing links to the actual content. Therefore the term "right to be delisted" will be used in this document when referring to the case. In the U.S., user-created content platforms have been the focus in many of the recent law and policy debates. Overall, several case studies indicate a potential shift of attention in law and policy-making towards heavily algorithm-based intermediaries.

While lawmakers around the world realize that intermediaries play a special role, they tend not to form strict categories and define such services as they used to define broadcasting. If there are specific rules, they often link to abstractly defined actions (such U.S. safe harbor rules and the Marco Civil, for example). The European E-Commerce Directive is a hybrid that attempts to define types of services based on abstract prototypes. The various prototypes in mind ("caching" providers, host providers, access providers) might be one reason for the challenges with this approach to categorizing intermediaries.

Finally, the case studies demonstrate how law and policymakers, regulators, and Courts in different parts of the world continue to struggle with the task of framing the specific functions that different types of intermediaries fulfill. In some instances, the functional approach is avoided altogether and replaced by more familiar questions of definition, as in the case of the recent CJEU ruling. Similarly, the possible effects of interventions are an area of concern and debate given the dynamic nature of the service ecosystem.

III. Governance Structures and Models

A. Overview

The different systems for intermediary governance can be divided into two very broad groups. First, there are systems where intermediaries are explicitly addressed, and where there is a governance system especially designed to deal with intermediaries. Second, there are systems where general rules are applied to intermediaries.

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

[11] Google Spain SL, Google Inc. v Agencia Española De Protección De Datos (AEPD), Mario Costeja González. European Court of Justice. 13 May 2014. Europa.eu. European Union, n.d. Web. 9 Dec. 2014. http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text&pageIndex=0&part=1&mode=DOC&docid=152065&occ=first&dir&cid=437838.

The significance of this distinction becomes apparent when analyzing the situation in Brazil before and after the Marco Civil came into force. Before the enactment of the Marco Civil, decisions on the liability of online intermediaries were influenced by three completely different understandings applied by Brazilian Courts.[12] One understanding led to an exemption of the provider from any liability for third party behavior; a second interpretation enforced a stricter liability regime grounded in the concept of risk of the providers' activity; and a third would trigger the liability of the provider to the existence of culpability on its part.[13] With the Marco Civil now in force, there is a special civil liability regime for intermediaries. However, it is too soon to foresee what rules the Courts will apply in specific cases based on the new law, and what types of intermediaries will be covered. However, though it is unclear how this will be applied in practice, at least there is now a coherent regulatory structure within Brazilian law.

The U.S. can serve as an example of a system with an explicit and far ranging special regulatory framework for intermediaries. Section 230 of the Communications Decency Act and Section 512 of the Digital Millennium Copyright Act[14] are pivotal pieces of regulation constituting a "safe harbor" for online intermediaries. The same is – at least in principle – true in the European Union, where the E-Commerce Directive[15] provides specific liability exemptions for online intermediaries. However, due to the limited scope of the exemption (injunctions are, for example, not covered by the regime) and – to some degree – uncertainty about how to apply the exemptions, European harmonization could not prevent the emergence of a rather fragmented system regarding intermediary liability.[16]

Studying the country cases presented here leads to the insight that different types of conflicts are predominant in different countries. While in Vietnam – and to some extent in Thailand and India – intermediaries mainly face takedown requests on grounds of state interest (in a broad sense, including the protection of the honor of the king in Thailand), in most of the other countries examined in this study it is user-user divergences that fuel the majority of conflicts. The first pattern may stem from a more interventionist approach of some governments; however, it may also be based on the differing strengths of personal rights and different cultures of the complainants in the countries examined. It is interesting to note that claims based on copyright are dealt with by a separate liability system in basically all of the countries covered by this study.

---

[12] Lemos, Ronaldo, and Carlos Affonso Pereira De Souza. "Online Intermediaries Case Studies Series: Brazilian Courts and the Internet – Rulings Before and After the Marco Civil on Intermediary Liability", The Global Network of Internet & Society Research Centers (2015), 2.

[13] Lemos, Ronaldo, and Carlos Affonso Pereira De Souza. "Online Intermediaries Case Studies Series: Brazilian Courts and the Internet – Rulings Before and After the Marco Civil on Intermediary Liability", The Global Network of Internet & Society Research Centers (2015), 2.

[14] 47 U.S. Code § 230 - Protection for private blocking and screening of offensive material; http://www.gpo.gov/fdsys/granule/USCODE-2011-title47/USCODE-2011-title47-chap5-subchapII-partI-sec230/content-detail.html.

[15] European Parliament. *Directive 2000/31/EC, "Directive on Electronic Commerce,"* European Union. June 8, 2000, http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=CELEX:32000L0031.

[16] Angelopoulos, Christina. *Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe*. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, November 28, 2013. http://papers.ssrn.com/abstract=2360997.

Another relevant distinction is whether a liability regime provides a safe harbor for intermediaries or not. Section 512 of the Digital Millennium Copyright Act (DMCA) in the U.S. is probably the most prominent example of a safe harbor clause. The basic rule here is that if there is no content curation, there is no liability. Thus, under the DMCA, the way that providers treat content is key. To some extent there is a safe harbor for intermediaries that do not exercise editorial control under the Indian IT Act.[17] Considering algorithmic journalism and similar developments, it will become rather difficult to draw such distinctions regarding curation in future.

The above-mentioned safe harbor clause in the E-Commerce Directive of the EU shows that not all harbors are equally protected against the strong wind of third-party claims. The directive defines different types of intermediary roles, and categorization into one of these roles typically leads to a provider being held not liable. Whether search engines fall into one of those categories and can consequently profit from safe harbor provisions is not entirely clear. However, while the explicit objective of the regulation was to create a safe harbor, especially to promote innovation in Europe, there are only limited cases in which the directive in fact provided such a "safe harbor."[18]

Another significant characteristic of any intermediary governance system is whether it establishes a notice-and-take-down procedure or not, and whether this procedure is set up as a condition for obtaining optional safe harbor protection or as a mandatory test of liability (i.e., failure to respond to a lawful notice immediately triggers liability). There can be an explicit regime, like in India,[19] or a situation like in Europe, where the CJEU ruling on data protection and search engines[20] resulted in a de-facto notice-and-take-down-procedure without a clear legal basis. The CJEU claims that search engine providers are controlling data processing when a user searches for a name of an individual, and that they must consider requests to delist names from search results. The decision is based on the European Data Protection Directive and answers questions submitted by a Spanish Court. Since it enables any person to request that a link be removed from search results, the ruling has been associated with the "right to be forgotten." This controversial judgment[21] requires search engine operators to establish a notice-and-take-down-procedure to comply with the European data protection framework.

B. Focus Areas

Internet liability regimes can serve as a model for contextual regulation. Laws do not regulate the behavior of an operator or an intermediary directly by prohibiting or ordering a specific

[17] Arun, Chinmayi, and Sarvjeet Singh. "Online Intermediaries Case Studies Series: Online Intermediaries in India", The Global Network of Internet & Society Research Centers (2015), 8-9.
[18] For the effect of the safe harbor clause (and its limits) on a European level see in particular Case C- 324/09, L 'Oréal v eBay, 12 July 2011, Case C-70/10, Scarlet v SABAM, 24 November 2011 and Case C- 360/10, SABAM v Netlog, 16 February 2012.
[19] Arun, Chinmayi, and Sarvjeet Singh. "Online Intermediaries Case Studies Series: Online Intermediaries in India", The Global Network of Internet & Society Research Centers (2015), 21.
[20] Google Spain SL, Google Inc. v Agencia Española De Protección De Datos (AEPD), Mario Costeja González. European Court of Justice. 13 May 2014.
[21] Kuczerawy, Aleksandra, and Ausloos, Jef. "Online Intermediaries Case Studies Series: European Union and Google Spain", The Global Network of Internet & Society Research Centers (2015), 19-20.

behavior.[22] Rather, the core of a liability regime is generally a set of conditions under which the operator will be held liable for third party content. Depending on mechanisms for enforcement and implementation, these regimes can lead to specific governance structures being formed within the operator of an intermediary, such as a notice-and-take-down-procedure to deal with user-user-conflicts on an online platform. Most countries examined in the case studies do not directly govern intermediaries but rather govern them indirectly via mechanisms of contextual regulation. While licensing regimes exist in some jurisdictions (Thailand can serve as an example),[23] it is noteworthy that they are reportedly used less for direct regulation in the traditional sense – for instance via licensing conditions – but rather as an enforcement mechanism.

The outcome of such indirect contextual regulation very much depends on the incentives and disincentives created by the system. For the functioning of an intermediary governance system, setting the right incentives is key. First and foremost this is true for the operator of the intermediary. The case of Korea[24] demonstrates that this is a difficult task in the complex environment defined by Internet regulation. The clause in the respective law in Korea[25] mentioning "temporary action" does create an incentive for the operator of an intermediary to remove content after having received notice, regardless of whether the content is legal or illegal. While this does not seem to be the intent of the law, it is rational for intermediary operators to act this way if they want to avoid liability. Looking at incentives created by the system, it is instructive to look at the users' end as well. The notice and-take-down system in Turkey creates greater incentives for users who believe his or her rights have been infringed upon to file a lawsuit directly with the Courts, rather than use the notice-and-take-down-system.[26] Obviously there is the risk of undesirable secondary effects in this situation because it is hard for a lawmaker to anticipate the actions of intermediary operators, if the lawmaker even tries to do this – which is not always the case with liability rules. In India, the Supreme Court will hear a case in the spring of 2015 regarding the rules that the government enacted under the safe harbor clause, which have been criticized for creating incentives to remove all content – illegal or legal – in the event of a notice.[27]

This reflection about incentives already focused on the different actors in a governance system. Looking at the governance structure at large, which emerges from – or is at least influenced by – a liability regime, reveals the structure of rules and the roles of different actors in such a system. In many cases the structure does not seem to be the result of a regulatory strategy, but a result of

[22] See Baldwin, Robert, and Martin Cave. *Understanding Regulation: Theory, Strategy, and Practice*. Oxford: Oxford University Press, 1999.
[23] Ramasoota, Pirongrong. "Online Intermediaries Case Studies Series: Online Intermediary Liability in Thailand", The Global Network of Internet & Society Research Centers(2015), 3.
[24] Park, Kyungg-Sin. "Online Intermediaries Case Studies Series: Intermediary Liability – Not Just Backward but Going Back", The Global Network of Internet & Society Research Centers (2015).
[25] 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), 6.
[26] Beceni, Yasin and Nilay Erdem. "Online Intermediaries Case Studies Series: Turkey (eBay Case)", The Global Network of Internet & Society Research Centers (2015), 12.
[27] cf. Arun, Chinmayi, and Sarvjeet Singh. "Online Intermediaries Case Studies Series: Online Intermediaries in India", The Global Network of Internet & Society Research Centers (2015).

the interplay of different actions. Take the CJEU ruling – the search engine case – as an example again.[28]

The CJEU decision can be seen as European institutions showing Google its limits. However, in doing so, the ruling moves the responsibility for deciding user-user-conflicts – i.e. conflicts between the person affected vs. the owner of the web page that contains the information about that person – to the search engine operator, since the operator is responsible under the data protection regulation for its search results. Any decision by Google can, of course, be subject to scrutiny by the data protection officer or the Courts, however, the initial decision remains with Google. Not only that, in absence of more detailed criteria – in the directive or in the Court's reasoning – regarding how to balance the interest of the person that wants a link removed and the interest of the owner of the respective web page or the general public at large to have access to this web page, Google has to come up with rules regarding how to solve such conflicts and balance the rights involved. Unintentionally the CJEU has created a mandatory notice-and-take-down-procedure, the rules of which are governed by search engines.

This also tells the story about the role of another type of actor in the governance system: the Courts. While the CJEU ruling on search engines is a very special case, in many countries we can see the relevance of single Court's decisions in shaping the given intermediary governance system. What we can learn from studying this aspect is that it puts a burden on the Courts to develop a coherent liability system in this complex environment (remember the three different ways to apply the general liability rules in Brazil). Furthermore, the Courts with their procedures and instruments to gain and *process knowledge* are not designed to anticipate the secondary effects of their judgments. The incentives created by judgments and the governance structure emerging from this cannot easily be anticipated by Courts.

It has already been mentioned that most of the intermediary governance systems contain notice-and-take-down-procedures – be it intentionally designed, as a de facto development, an optional procedure for obtaining a safe harbor, or a mandatory test of intermediary liability – as an essential part of their structure, and there is a great variety of such systems. The fact that notice-and-take-down has become a very "fashionable" way to treat user-user conflicts on intermediary platforms has been criticized from a normative standpoint, to the extent that the procedure becomes a mandatory test of intermediary liability. The report by Frank La Rue[29] clearly states that an operator of an intermediary should not be put in the position to decide whether to remove content or not; it should be up to an independent Court or another independent body within a government to judge the legality or illegality of making content available. A mandatory notice-and-takedown procedure is likely to violate La Rue's recommendation.

Two aspects of a notice-and-take-down-procedure seem to be significant. The first is the design of the procedure; models range from having no procedural requirements at all to models with

[28] Google Spain SL, Google Inc. v Agencia Española De Protección De Datos (AEPD), Mario Costeja González. European Court of Justice. 13 May 2014. For more detail see: Kuczerawy, Aleksandra, and Ausloos, Jef. "Online Intermediaries Case Studies Series: European Union and Google Spain", The Global Network of Internet & Society Research Centers.

[29] La Rue, Frank. "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression." United Nations Office of the High Commissioner of Human Rights. 2013. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

fine-tuned procedures set out in a bylaw, such as that established by the administration in India.[30] The other significant aspect is the treatment of the operator of the affected web site and the general interest in easy access to online information. Only very rarely is there a mandatory notice to the operator of the web page before a take-down happens,[31] or is a structured appeal procedure launched by the operator in question.

Depending on the nature of the claim, the procedure adopted by an intermediary to deal with notices can be an automated system like ContentID by YouTube, which allows YouTube to identify copyright protected content and have it removed, or a manual system, like the procedure which as been established by Google to deal with the over 160,000 requests as of end of October 2014 following the CJEU ruling. Alternatively, hybrid systems exist where a large amount of potentially protected content will be dealt with automatically, but the hard cases are treated manually.

IV. Role of the Government

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.

[30] Arun, Chinmayi, and Sarvjeet Singh. "Online Intermediaries Case Studies Series: Online Intermediaries in India", The Global Network of Internet & Society Research Centers (2015), 5.

[31] U.S. 17 U.S.C. 512(g)(2)(A) (g) Replacement of Removed or Disabled Material and Limitation on Other Liability.—(1) No liability for taking down generally. — Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.
(2) Exception. — Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice provided under subsection (c)(1)(C), unless the service provider — (A) takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material; 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), 11-13.

A. Functions

The case study series reveals that governments have varying motives for regulating online intermediaries. In broad terms of regulatory theory,[32] 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,[33] 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.[34] While the historic motives for introducing these liability limitations were rather nuanced (in the case of the U.S. Communications Decency Act [CDA], for instance, the lawmaker wanted to enable content self-regulation by online intermediaries without exposing them to liability),[35] 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).[36]

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

[32] See generally, e.g., Baldwin, Robert, and Martin Cave. *Understanding Regulation: Theory, Strategy, and Practice*. Oxford: Oxford University Press, 1999.

[33] 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).

[34] 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.

[35] 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.

[36] 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.

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-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)[37] 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.[38] The licensing regime in Vietnam imposes hard constraints under which online intermediaries have to operate, to give another example from the case study series.[39]

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.

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

[37] Ramasoota, Pirongrong. "Online Intermediaries Case Studies Series: Online Intermediary Liability in Thailand", The Global Network of Internet & Society Research Centers (2015), 4.
[38] Beceni, Yasin and Nilay Erdem. "Online Intermediaries Case Studies Series: Turkey (eBay Case)", The Global Network of Internet & Society Research Centers (2015).
[39] 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).

governance framework.[40] 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.[41]

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.[42] 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.[43]

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.[44] 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

[40] 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).
[41] 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.
[42] 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).
[43] 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).
[44] 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.

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.[45] In contrast, the governance models in India, Korea, and Thailand create asymmetric incentive structures, where intermediaries are incentivized to take down content in order to avoid liability, even if it results in over-compliance.[46]

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.[47] 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.[48] 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 from Thailand, Turkey, and India demonstrate.[49]

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

[45] 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.

[46] 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).

[47] 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).

[48] 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.

[49] 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).

over private mechanisms.[50] The contrast between automated compliance and enforcement in response to copyright issues on YouTube, versus the human and labor-intense review of takedown requests that attempt to balance user interests under the CJEU's right to be delisted, highlights yet another important dimension of the cost argument when it comes to online intermediary governance.

V. General Observations

A. Evolutionary Paths

The analysis so far has focused on the governance structure and was therefore based on more of a static view. Another perspective from which intermediary governance can be analyzed is the process of development. A first and rather obvious observation is that the political discourse in the countries covered by this study recognized the relevance of intermediary governance at different points of time. So it may be fair to say that the systems are not equally mature. The U.S. appears to have been fast in addressing the issue, and as a result the system has been in force for several years and proven to be relatively stable. Other countries are still in the process of designing a system.

A less obvious, but also significant aspect seems to be the cultural context. Protecting the honor of the king in Thailand, for example, is deeply rooted in Thai society and has to be guaranteed against defamation online and offline. Consequently the role of all actors, including operators of intermediaries, is addressed. Countries with an aspiration to govern society more strictly than a western democracy face the dilemma of finding a way to govern the Internet – including intermediaries – without tampering with innovation and the economic potential of the Internet. Vietnam[51] can serve as an example of a country grappling with such a balance. The U.S., additionally, bases their regulation on a shared understanding on the importance of freedom of speech; thus the cultural context again is key.

What we can see in the development of intermediary governance, as well as in other sectors of regulation, is that sometimes single events change the development path. A significant event has been the CJEU ruling on search engines, which has fuelled the debate on the responsibility of operators of intermediaries in Europe and beyond. This can even affect the construction of the relationship of whole bodies of law, like the right to private life on the one hand and data protection on the other, which has come into the spotlight as a result of the CJEU ruling. Furthermore, general political developments in a country, like the Coup in Thailand, can affect the regulations of intermediaries and lead to restrictions on free speech.

Another driver of change might be developments in the international arena. While not necessarily visible in the present case studies, standards for intermediary liability in particular might be the subject of agreements between countries in the context of bi- or multilateral trade agreements. The negotiations on the Trans-Pacific Partnership Agreement serve as a recent case

[50]Beceni, Yasin and Nilay Erdem. "Online Intermediaries Case Studies Series: Turkey (eBay Case)", The Global Network of Internet & Society Research Centers (2015), 13.
[51] 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).

in point.[52] Other important impulses at the international level might come from Human Rights frameworks (of particular importance in this context is the Declaration of Human Rights and the International Covenant on Civil and Political Rights), and also global multi-stakeholder efforts such as NETmundial.[53]

B. Interplay Between Constitutional Rights and Intermediary Liability

The CJEU decision highlights another relevant aspect of intermediary governance systems, which is the relationship between intermediaries' liability and constitutional rights. The ruling has been criticized for not sufficiently taking freedom of speech and freedom of information into consideration.[54] It is not unlikely that cases triggered by the decision of the European Court will lead to lawsuits on which national constitutional Courts, as well as the European Court on Human Rights, will have to decide. At the same time, the liability regime in India has been challenged due to constitutional reasons, and the same is true for Korea. At least two aspects are noteworthy when it comes to the constitutional rights aspect of intermediary liability.

The first is that liability systems cannot trust the publisher of a web page to stand up for his or her right to freedom of speech if he/she is not informed about the take-down, if it is costly to respond, or he/she is not interested in pursuing the matter. Furthermore, the general interest in easy access to information on the Internet is not protected under freedom of information clauses because it is framed as a subjective not objective right. However, some Courts have emphasized the role of the Internet in this respect.[55] In terms of actors, there is an imbalance when there is a situation where there is a person highly interested in getting the content removed on one side and a potentially uncommitted person on the other – if any.

Secondly, the role of the operator of an intermediary is under consideration. On one hand, the operator might be enjoying freedom of speech privileges itself[56] – but the conditions under which this is the case are not easy to construe. On the other hand, the operator might be a powerful entity that decides the accessibility to a piece of information should be bound to respect freedom of speech vis-à-vis the users as well. The debate about the implication of these constitutional issues has just started.

---

[52] On the role of intermediary liability in trade, see, e.g., "Harmonizing Intermediary Immunity for Modern Trade Policy," The Internet Association, May 5, 2014. http://Internetassociation.org/wp-content/uploads/2014/05/May-2014-Section230.pdf.

[53] See "The Manila Principles On Intermediary Liability: Version 0.9," Organization,, December 1, 2014, https://docs.google.com/document/d/1kAkqgt3cRb65d8ik6vWYgpk6DYpP8ABA43ljgDiGOf8/edit?usp=sharing

[54] "Google Starts Removing Search Results Under Europe's 'Right to Be Forgotten.'" *WSJ*. http://www.wsj.com/articles/google-starts-removing-search-results-under-europes-right-to-be-forgotten-1403774023.

[55] E.g. the ECtHR: "In the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the sharing and dissemination of information generally (accessible) (Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2), nos. 3002/03 and 23676/03, § 27, ECHR 2009, and Ashby Donald and Others v. France, no. 36769/08, § 34, 10 January 2013).

[56] "Volokh, Eugene. "First Amendment Protection for Search Engine Search Results." The Volokh Conspiracy, May 9, 2012. http://volokh.com/wp-content/uploads/2012/05/SearchEngineFirstAmendment.pdf.

VI. Conclusion

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, 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 socio-economic 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.[57] 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.[58]

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.

[57] 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-online-intermediaries-and-liability-system-not-yet-fit-purpose.

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

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.

Appendix A:
European Union and Google Spain

NoC Online Intermediaries Case Studies Series: European Union and Google Spain[1]

Aleksandra Kuczerawy and Jef Ausloos
Interdisciplinary Centre for Law & ICT (ICRI), KU Leuven

Editorial Note: Context, Character, and Purpose of the Case Study

This case study is part of a globally coordinated, independent academic research project by the Global Network of Interdisciplinary Internet & Society Research Centers (NoC). Facilitated by the Berkman Center for Internet & Society at Harvard University, the project is the first output of a larger policy-oriented research initiative that examines the rapidly changing landscape of online intermediary governance at the intersection of law, technology, norms, and markets. In concert with other research projects, it seeks to develop criteria, comparative methods, and a shared data repository, and to compile insights and lessons learned across diverse communities of knowledge aimed at informing and improving Internet policy-making globally.

The initial research output consists of a case study series exploring online intermediary liability frameworks and issues in Brazil, the European Union, India, South Korea, the United States, Thailand, Turkey, and Vietnam, and a synthesis paper that seeks to distill key observations and provide a high-level analysis of some of the structural elements that characterize varying governance frameworks, with a focus on intermediary liability regimes and their evolution.

The authors of these case studies have participated in a multi-step process of in-person consultations and remote collaborations among a global team of researchers from the Network of Centers. Additionally, the case studies are based on a set of broader questions regarding the role of online intermediaries in the digital age.[2]

The research effort is grounded in a diversity of global perspectives and collaborative research techniques, committed to objective and independent academic standards, and aspires to be useful, actionable, and timely for policymakers and stakeholders. More broadly, the Network of Centers seeks to contribute to a more generalized vision and longer-term strategy regarding the role of academic research, facilitation and convening, and education and communication in the Internet age. For additional information on the initiative, please contact Urs Gasser, Berkman Center for Internet & Society, at ugasser@cyber.law.harvard.edu

---

[1] Part of the research leading to these results has received funding from the European Community's Seventh Framework Program for research, technological development and demonstration in the context of the EXPERIMEDIA project (www.experimedia.eu) under grant agreement no: 287966 and the REVEAL project (revealproject.eu) under grant agreement no: 610928, as well as the Flemish research institute iMinds (www.iminds.be).

[2] The process is documented at: "Online Intermediaries: Functions, Values, and Governance Options", The Global Network of Internet & Society Research Centers, 2014 https://drive.google.com/file/d/0B_ToTBKP5ITVWTl0UzV0U3B2RlU/view?usp=sharing.

Abstract: This paper provides an overview of the legal framework governing the liability of online intermediaries in the European Union (EU). The E-Commerce Directive undoubtedly constitutes the key legal instrument targeting online intermediaries on the EU-wide level. After outlining the key provisions in this Directive, the paper will analyze the *Google Spain* ruling as a case study.[3] This ruling is particularly interesting for two reasons. First of all, it involves a type of intermediary (search engine) whose legal position is largely undefined at the EU level. Secondly, the *Google Spain* case concerns the position of search engines vis-à-vis the personal data they process. In this regard, it is an ideal case study with which to evaluate the interaction between the intermediary liability regime and data protection law. Additionally, it provides food for thought with regard to the role of intermediaries in the governance of the Internet.

[3] CJEU, Google Spain, C-131/12, Grand Chamber, 13.05.2014, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=264438.

Table of Contents

I. Introduction

After introducing the liability regime for online intermediaries in the EU, this working paper makes a deep-dive into the particular position of search engines. The Court of Justice of the EU (CJEU) has recently issued a ruling obliging search engines to de-link certain results when person-names are used as search terms. The so-called *Google Spain* Case also highlights the important discussion on the interaction between data privacy laws and intermediary liability exemptions. Using this case as the thread throughout the second half of the paper, we identify the core issues that are relevant and need further research.

II. EU Regime on Liability of Intermediaries – E-Commerce Directive 2000/31/EC

In the European Union, Directive 2000/31 regulates the liability of online intermediaries on certain legal aspects of information society services, in particular electronic commerce in the Internal Market (E-Commerce Directive, ECD).[4]

The E-Commerce Directive was proposed by the European Commission in 1998, and signed by the European Parliament and the Council of the EU in June 2000. Member States had until January 2002 to implement the Directive into their national legal orders.[5]

As observed in the preamble to the Directive, the development of information society services within the Community is hindered by a number of legal obstacles that make the exercise of the freedom of establishment and the freedom to provide services less attractive.[6] Moreover, "these obstacles arise from divergences in legislation and from the legal uncertainty as to which national rules apply to such services."[7] The goal of the Directive, therefore, is to create a legal framework to ensure the free movement of information society services between Member States. The Directive aims to achieve this by realizing two main objectives. In the first instance, it seeks to remove certain legal obstacles hampering the development of electronic commerce within the internal market. At the same time, it is also aimed at providing legal certainty and ensuring consumer confidence towards electronic commerce. The development of electronic commerce was considered a crucial factor that would stimulate economic growth and investment in innovation by European companies, and which could also enhance the competitiveness of European industry.[8]

---

[4] Directive 2000/31 of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178, 17.07.2000, 1-16.

[5] See more in: First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on the Directive on Electronic Commerce, COM(2003) 702 final, Brussels, 21.11.2003;

[6] Freedom of establishment (articles 49 to 55 TFEU) and freedom to provide services (56 to 62 TFEU) are intended to guarantee the mobility of businesses and professionals within the EU (See: recital (5) to the E-Commerce Directive). See more at: http://www.europarl.europa.eu/aboutparliament/en/displayFtu.html?ftuId=FTU_3.1.4.html; See the full text of the Treaty on the Functioning of the European Union at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012E/TXT.

[7] Recital (5) to the E-Commerce Directive.

[8] Recital (2) to the E-Commerce Directive.

The Directive only partially succeeded in achieving its objectives. Since the introduction of the Directive, e-commerce in the EU has generally grown.[9] However, it is still less advanced than in the United States and the Asia-Pacific.[10] For a long time cross-border activity remained low,[11] although steady growth can be observed in the last few years.[12] Nonetheless, the European Commission has expressed the view that more needs to be done in order to achieve the Directive's full potential.[13]

The E-Commerce Directive regulates several aspects of information society services, including freedom of services, the treatment of electronic contracts, and liability issues for third party content, among others. In this section we briefly present the scope of the Directive before focusing more extensively on the intermediary liability provisions.

A. Scope

The E-Commerce Directive applies to "information society services." Such services are defined as '"…any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" (art. 2.a E-Commerce Directive). The notion of "information society services" covers a wide range of services. Many of the economic activities that take place online fall under the scope of the E-Commerce Directive. Examples of the services falling under this broad definition can be found in Recital (18) to the Directive. They may include (in so far as they represent an economic activity): online contracting, services providing transmission of information via communication networks, services providing access to a communication network, hosting of information, as well as services that do not give rise to on-line contracting, e.g. those that offer online information or commercial communications or those that provide tools allowing for search, access and retrieval of data.[14]

The key elements in determining whether or not a particular service can be qualified as an information society service are as follows:

---

[9] Commission Communication to the European Parliament, The Council, The Economic and Social Committee and The Committee of Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services {SEC(2011) 1640 final} http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:EN:PDF, p. 3.

[10] Ibid. p.3.

[11] 5th Consumer Conditions Scoreboard, Consumers at home in the single market, European Commission, March 2011, http://ec.europa.eu/consumers/consumer_research/editions/cms6_en.htm

[12] 9th Consumer Conditions Scoreboard, Consumers at home in the single market, European Commission, July 2013, http://ec.europa.eu/consumers/archive/consumer_research/editions/docs/9th_edition_scoreboard_en.pdf

[13] Commission Communication to the European Parliament, The Council, The Economic and Social Committee and The Committee of Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services {SEC(2011) 1640 final} http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:EN:PDF, p. 6. For the analysis of the remaining obstacles to the development of the e-commerce in the EU see also Commission Staff Working Document Online services, including e-commerce, in the Single Market, Brussels, 11.1.2012 SEC(2011) 1641 final http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf; and Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC), available at: http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf.

[14] See Recital (18) to the E-Commerce Directive for more examples.

- Remuneration[15];
- Distance;
- Electronic means;
- Individual request of a recipient[16].

The E-Commerce Directive also excludes a number of services and legal issues from its scope such as, for example, questions covered by the Data Protection Directive (art. 1(5).b).[17]

B. Liability Exemptions for Intermediaries

The E-Commerce Directive regulates the liability of intermediary service providers in Section 4. This part of the Directive contains provisions introducing liability exemptions for certain types of intermediary services. Only three types of services are covered, namely 'mere conduit' (article 12), 'caching', (article 13) and 'hosting' (article 14). In order to benefit from these exemptions, providers of such services must comply with the conditions of each article.

The liability provisions of the E-Commerce Directive reconciled two main arguments in the debate taking place between the Internet industry and EU policy makers at the time. On one hand, there was the concern that if intermediaries were to be held liable for third party content on similar grounds as 'publishers,' it could restrain service providers from entering the market.[18] On the other hand, the European Commission recognized the role that online intermediaries could play in limiting illegal online content and, through that, improved public trust and confidence in the Internet as a safe space for economic activity.[19] The balance that was reached was meant to stimulate growth and innovation of the newly born technology and provide positive incentives for further development, which would effectively contribute to reaching the goals delineated in the E-Commerce Directive.[20]

The scope of the liability exemptions in the E-Commerce Directive is horizontal. This means that the liability exemptions cover various types of illegal content and activities (infringements on

[15] The element of remuneration does not necessarily refer to the specific way in which the service is financed. Rather than that, it refers to the existence of an economic activity or an activity for which an economic consideration is given in return. Information society services therefore extend to services which are not remunerated by those who receive them. This means that a service financed through advertising, such as for example social networking site or a search engine, would be classified as an information society service.

[16] The element of "individual request of a recipient of services" covers an activity of visiting a website. The transmission of data is initiated on demand, by an individual 'requesting' the URL or following a link.

[17] Additionally, the Directive does not apply to: issues related to taxation; questions relating to agreements or practices governed by cartel law; the activities of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority. See article 5.1 E-Commerce Directive.

[18] OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communication Policy, The Role of Internet Intermediaries In Advancing Public Policy Objectives, Forging partnerships for advancing public policy objectives for the Internet economy, Part II, 22.06.2011, p. 12.

[19] Ibid., p. 12.

[20] See Recitals 1-6 of the E-Commerce Directive.

copyright, defamation, content harmful to minors, unfair commercial practices, etc.) and different kinds of liability (criminal, civil, direct, indirect).[21]

If the conditions for being exempt from liability are not met, this does not mean that the intermediary is per se subject to liability. The effect is that the intermediary can no longer rely on the immunity provided by the Directive. The question of liability is then determined under the applicable material law specific for the type of infringing content in each Member State.[22]

1. Mere Conduit

Art. 12 targets traditional Internet access providers and backbone operators. The liability exemption provided in this provision refers to providers of 'mere conduit' services, which are described as:

- Services which consist of the transmission in a communication network of information provided by a recipient of the service ('transmission services'); and
- Services which consist of the provision of access to a communication network ('access services').

Recital (42) further stipulates that the exemptions provided by the Directive apply only to cases "where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network (…)."[23] It further elaborates that such activities are of a mere technical, automatic, and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information it transmits or stores.[24] The services described in art. 12 are sometimes compared to postal services, which are similarly not held liable for the illegal content of a letter.[25]

The 'mere conduit' exemption of liability only applies on the condition that the service provider:

- (a) Does not initiate the transfer of data ;
- (b) Does not select the recipient of the data; and

---

[21] Helberger N., et al., 'Legal Aspects of User Created Content' in IDATE, TNO, IViR, User-Created Content: Supporting a Participative Information Society, Study for the European Commission (DG INFSO), December 2008, p. 220, available at: http://www.ivir.nl/publications/helberger/User_created_content.pdf.

[22] Van Eecke P., Truyens M., Legal analysis of a Single Market for the Information Society, New rules for a new age? a study commissioned by the European Commission's Information Society and Media Directorate-General, November 2009. Chapter 6: Liability of Online Intermediaries, p.10. Available at: http://ec.europa.eu/information_society/newsroom/cf/document.cfm?doc_id=842.

[23] Recital (42) to the E-Commerce Directive.

[24] While recital (42) purports to address all of the exemptions of the Directive, one might argue that the scope of this part of the recital should be limited to the transmission and access services identified in articles 12 and 13. After all, the exemption for hosting identified in art. 14 does not limit its scope to either transmission or access services (see also Montéro, E., 'Les responsabilités liées au web 2.0', Revue du Droit des Technologies de l'Information 2008, n° 32, p. 367). However, the ECJ has held recital (42) equally applicable to hosting services: see European Court of Justice, Joined Cases C-236/08 to C-238/08, 23 March 2010 (Google France and Google v. Louis Vuitton Malletier a.o.), paragraphs 113-114.

[25] Lodder A., 'Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, in Lodder A. and Kasspersen (eds.), eDirectives: Guide to European Union Law on E-commerce – Article by Article Comments, Kluwer Law international, 2002, p. 87.

- (c) Does not select or modify the transmitted data.

The liability exemption for mere conduits also extends to the automatic, intermediate, and transient storage of the information transmitted. This is the case if the storage takes place for the sole purpose of carrying out the transmission in the communication network. Moreover, the information cannot be stored for any period longer than is reasonably necessary for the transmission (art. 12.2).

Despite the lack of liability of the service provider (when the conditions are met), national courts and administrative authorities may direct prohibitory injunctions towards a provider of a 'mere conduit' service. Such injunction must be in accordance with the law of the Member State where the case is decided (Article 12.3).[26]

2. Caching

The second liability exemption provided by the E-Commerce Directive applies to the 'caching' of information. The provision is targeted at providers of so called 'proxy-servers.'[27]

Caching is defined as "the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request."[28] This exemption covers only information society services which consist of the transmission in a communication network of information provided by a recipient of the service ('transmission services') (art. 13.1).[29] Just as 'mere conduits,' providers of this type of service can only be exempted from liability if they are in no way involved with the information transmitted (recital (43)). In addition, the following five conditions must be met in order for a service provider to benefit from the caching exemption (art. 13.1):

- The (service) provider may not modify the information as it would deprive him of the position of the intermediary;

---

[26] The matter of injunction towards an Internet service provider was discussed recently by the Court of Justice of the European Union (CJEU) in the UPC Telekabel. The case concerned an injunction for the Internet service provider (UPC Telekabel) to block access of its customers to a website making available to the public copyright infringing materials. The Court ruled that an injunction ordering blocking access to such website does not have to specify the measures to be taken by the ISP. As long as the ISP takes all reasonable measures to achieve the result defined in the injunction, it shall not be a subject to penalties for breach of the injunction. These measures should have the effect of preventing unauthorized access to the protected material or, at least, of making it difficult to achieve and of seriously discouraging Internet users. At the same time such measures should appropriately balance other rights at stake. See par. 64 of the ruling. See: CJEU, Case C 314/12, 27 March 2014, (UPC Telekabel Wien).

[27] Van Eecke P., Truyens M., Legal analysis of a Single Market for the Information Society, New rules for a new age? a study commissioned by the European Commission's Information Society and Media Directorate-General, November 2009. Chapter 6: Liability of Online Intermediaries, p.8.

[28] Article 13.1 to the E-Commerce Directive.

[29] When comparing the caching exemption with the exemption for transient storage under the 'mere conduit' rule of art. 12.2, the wording appears to be very similar. The key difference between the caching exemption for transient storage and the exemption for transient storage under the mere conduit provision therefore is the purpose for which the storage is taking place. See Lodder A., 'Directive 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, in Lodder A. and Kasspersen (eds.), eDirectives: Guide to European Union Law on E-commerce – Article by Article Comments, Kluwer Law international, 2002, p. 88.

- The provider has to comply with conditions on access to the information;
- The provider must update the information regularly in accordance with the generally recognized rules and practices in this area;
- The provider may not interfere with the lawful use of technology that is used to measure the use of information;
- The provider must remove the cached information immediately upon obtaining actual knowledge that the initial source of the information is removed, access to it has been disabled, or that a court administrative authority has ordered such removal or disablement.

The liability exemption for caching does not affect the power of courts or administrative authorities to issue prohibitory injunctions in accordance with the national legal system (art. 13.2).

3. Hosting

Article 14 of the E-Commerce Directive provides the third liability exemption for online intermediaries. This provision concerns information society services consisting of the storage of information provided by a recipient of the service at his request. Typically, it concerns webhosting services that provide web space to their users, where users can upload content to be published on a website (e.g. YouTube).[30]

The storage by the 'hosting' service providers differs from the storage carried out in the context of mere conduit or caching mainly in terms of the purposes for which the storage takes place. In contrast to mere conduit or caching services, such storage is not merely 'incidental' to the provision of the transmission or access services.[31] Storage may be provided for a prolonged period of time, and may also be the primary object of the service.[32] In comparison to mere-conduit and caching services, the level of passivity required from the providers of the hosting service is different.[33] The Court of Justice of the EU specified that in order to enjoy the benefit of

---

[30] Van Eecke P., Truyens M., Legal analysis of a Single Market for the Information Society, New rules for a new age? a study commissioned by the European Commission's Information Society and Media Directorate-General, November 2009. Chapter 6: Liability of Online Intermediaries, p.9.

[31] I. Walden in: Bullesbach A., Poullet Y., Prins C. (eds.), Concise European IT Law, Kluwer Law International Alphen aan den Rijn, 2005, p. 253.

[32] It has been said that this exemption was originally aimed at ISP's providing space on their Internet servers for third parties' websites, or bulletin boards or chat room services provided by the ISP itself (where the ISP only provides technical means for the users' communication without interfering with the content being communicated between the users) (see: S.S. Jakobsen, 'Mobile Commerce and ISP Liability in the EU', International Journal of Law and Information Technology 2010, vol. 19 no. 1, p. 44). However, the exemptions provided by the E-Commerce Directive are defined in functional terms (i.e. in terms of the activity being performed), not in terms of the qualification of the actor. While the European legislator arguably only envisioned providers whose services consisted mainly, if not exclusively, in the performance of operations of a strictly technical nature, the scope of the exemption may also be applied to other entities (provided the conditions set forth by art. 14 are met). As a result, the exemption may in principle benefit any type of service provider who stores content at the request of the recipient; including so-called 'web 2.0' service providers (see E. Montéro, 'Les responsabilités liées au web 2.0', Revue du Droit des Technologies de l'Information 2008, n° 32, 369-373).

[33] Van Eecke P., Truyens M., Legal analysis of a Single Market for the Information Society, New rules for a new age? a study commissioned by the European Commission's Information Society and Media Directorate-General, November 2009. Chapter 6: Liability of Online Intermediaries, p.9.

the liability exemption, a service provider's conduct must be neutral. The Court further defined neutrality as a conduct that is "technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores."[34]

Such service provider shall not be liable for the information stored, on the condition that:

- The provider is not aware of facts or circumstances from which the illegal activity or information is apparent – with regard to civil claims for damages, and he does not have actual knowledge of illegal activity or information – with regard to other claims (art. 14.1.a); or
- The provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information (art. 14.1.b).

Interestingly, the Directive introduces different levels of knowledge with regard to criminal and civil liability. For the former, 'actual knowledge' is required, while for the latter it is enough to establish 'constructive knowledge' of the service provider. It is not entirely clear, however, what the boundary is between these types of knowledge. For example, the interpretations of 'actual knowledge' range among the EU countries from knowledge obtained through a court order, to informal notice by a user, which, however, should be sufficiently substantiated.[35] Divergent case law across the EU shows that there is a lack of consistency in the interpretation of these terms and the following requirements for a valid notice.[36]

The exemption of article 14 does not apply when the recipient of the service is acting under the authority or the control of the provider (art. 14.2). For example, if the service provider is acting as an employer or supervisor of the service recipient, it will not qualify for the exemption if the content was introduced pursuant to its instructions.

Similarly, as in the case of the 'mere-conduit' and caching services, the liability exemption does not affect the possibility of a court or administrative authority, in accordance with Member States' regulations, requiring the service provider to terminate or prevent an infringement (art. 14.3).

Article 14.3, additionally, creates for Member States the possibility of establishing specific procedures governing the removal or disabling of access to information. The Directive does not provide any details for taking down or blocking access to content from article 14.1.b. In consequence, there are no procedures on how such processes should be handled by service providers, nor safeguards to ensure proportionality or due process of the removal or blocking.

---

[34] Court of Justice of the European Union, Joined Cases C-236/08 to C-238/08, 23 March 2010 (Google France and Google v. Louis Vuitton Malletier a.o.), paragraphs 113-114. The European Court of Justice addressed the issue of neutrality of hosting service providers also in the L'Oréal eBay case. The Court ruled that art. 14 of the Directive applies to hosting providers if they don't play an active role that would allow them to have knowledge or control of the stored data. Court of Justice of the European Union, Case C□324/09, 12 July 2011 (L'Oréal v. eBay), paragraphs 112 - 116.

[35] European Court of Justice (Grand Chamber), C□324/09, 12 July 2011, (L'Oréal SA and others).

[36] See for example: BGH, 23/09/2003, VI ZR 335/02; Dutch Supreme Court 25 November 2005, LJN Number AU4019, case number C04/234HR; M. Turner(ed.) & J. Llevat, "The Spanish Supreme Court clarifies the concept of actual knowledge in connection with ISP's liability", Comp LSR 2010, volume 26, issue 4, 440-441.

Procedural aspects were left entirely to the discretion of the Member States.[37] Some of the EU countries provided a more detailed regulation for the hosting exemption by introducing formal notification procedures ('Notice-and-Take Down procedures'). Many, however, opted for a verbatim transposition of the Directive, leaving this matter unattended.[38]

4. No General Obligation to Monitor

Member States may not impose on providers of services covered by articles 12, 13, and 14 (i.e. mere conduit, caching or hosting) a general obligation to monitor information they transmit or store (art. 15). The same provision states that they cannot introduce a general obligation to actively look for facts or circumstances indicating illegal activity.

An obligation to conduct general monitoring of content, if permitted, would counteract the limited liability paradigm.[39] This is because intermediary service providers actively seeking illegal activities would no longer be neutral and passive in nature. Moreover, a general monitoring obligation could lead to censorship and consequently have a negative impact on freedom of expression.[40]

The prohibition towards monitoring obligations refers solely to monitoring of a general nature. It does not concern monitoring obligations in a specific case, nor does it affect orders by national authorities in line with national legislation (Recital (47)).[41] The Directive also allows Member States to require hosting providers to apply duties of care, which can reasonably be expected from them (Recital (48)). Such duties of care, however, should only be introduced to detect and prevent certain types of illegal activities, foreseen by national law.[42] To the confusion of many, the Directive does not specify what exactly such duties of care entail. As a result, the boundary

---

[37] Also in recital 46, the Directive stipulates that the removal or disabling of access should be undertaken in observance of this right and of procedures established for this purpose at national level.

[38] First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on the Directive on Electronic Commerce, COM(2003) 702 final, Brussels, 21.11.2003;

[39] OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communication Policy, The Role of Internet Intermediaries In Advancing Public Policy Objectives, Forging partnerships for advancing public policy objectives for the Internet economy, Part II, 22.06.2011, p. 15.

[40] Ibid. p. 36. See also Council of Europe, Human rights guidelines for Internet Service Providers – Developed by the Council of Europe in co-operation with the European Internet Service Providers Association (EuroISPA), July 2008, p.3, available at: http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)009_en.pdf

[41] Application of art. 15 differs across the EU in case of injunctions. For example, in Germany a host may still be required to actively monitor his platform for further infringing activity. See more in T. Verbiest, Spindler G, et al., Study on the liability of Internet Intermediaries – General trends in Europe, Markt/2006/09/E, 12.11.2007, p. 85.

[42] Prohibition of the general monitoring obligation was addressed by the Court of Justice of the European Union in two cases, Scarlet v. Sabam and Sabam v. Netlog. Both cases concerned an obligation to install a filtering system in order to prevent sharing of copyright infringing files. Such request was initiated by the Belgian authors' association (Sabam) with regard to an Internet Service Provider (Scarlet), and to a Belgian social networking site (Netlog). The Court decided, in both cases, that an injunction requiring to install a filtering system for all information which is passing via its services or stored on its servers by its users would constitute a general monitoring obligation if it applies indiscriminately to all of the users; as a preventative measure; exclusively at the provider's expense; and for an unlimited period, and if it is capable of identifying electronic files containing musical, cinematographic or audio-visual work of which the applicant holds intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright. Court of Justice of the European Union, C-70/10, 24 November 2011 (Scarlet v. SABAM), and Court of Justice of the European Union, C-360/10, 16 February 2012 (SABAM v. Netlog).

between such duties and general monitoring is not clear. Recital (48), for this reason, can be seen as contradictory to art. 15.[43]

The prohibition of article 15 is addressed to the Member States' legislators. They are not allowed to introduce regulations that would require providers of the specified services to monitor the information they store or transmit. This does not mean that service providers cannot take up such activities on their own. The prohibition should not be read as a prohibition against service providers monitoring information. Most of the service providers in the EU do perform certain monitoring activities to maintain a 'civilized' environment on their service. Voluntary monitoring, however, can prove detrimental. Exercising too much control could compromise the neutral status of the intermediary and, in consequence, deprive them of the safe harbor protection. The EU intermediary regime does not contain a 'Good Samaritan-like' clause.[44] There is no provision which explicitly protects intermediaries from liability should their voluntary monitoring prove imperfect. As a result, service providers are careful not to shoot their own foot by being overzealous.

Article 15 (2) defines two additional obligations that Member States may impose upon information society service providers. The first provides Member States the possibility to require service providers to inform authorities about any alleged illegal activities of their users. Such notification would need to be given as soon as the provider becomes aware of the illegal activity. Secondly, Member States may also establish obligations on providers to disclose the identity of users with whom they have storage agreements. Establishing these obligations is not a requirement and is left to the discretion of the Member States.[45]

The regime laid out by the E-Commerce Directive has been in place for over two decades now, without any update or amendment. During this time, a number of issues have been identified with regard to its functions.[46] The review process of the Directive was, therefore, long awaited.

---

[43] Barceló R. J. and Koelman, K., 'Intermediary Liability In The E-Commerce Directive: So Far So Good, But It's Not Enough', Computer Law & Security Report 2000, vol. 4, pp. 231-239, p. 232.

[44] Such as, for example the one offered by the US CDA, Section 230 (c)(2).

[45] The possibility of introducing an obligation to disclose the identity of recipients was questioned in the Promusicae case (CJEU, C 275/06, 29 January 2008, Promusicae v. Telefonica de Espana). The request for preliminary ruling concerned questions whether Member States were required to introduce such an obligation in order to effectively protect copyrights. Moreover, a question was asked whether such obligation could pose a risk of infringement of a right to respect for private life of the users. The Court ruled that the Member States are not required to lay down an obligation to communicate personal data in order to ensure effective protection of copyright. Moreover, the Court stated that when transposing directives into national legal system a fair balance needs to be struck between the various fundamental rights protected by the Community legal order. In this case, the rights to protection of property, including intellectual property and the right to effective remedy with the right to protection of personal data, hence to private life. No guidelines how to struck such balance were provided by the Court. See more: F. Coudert, E. Werkers, In The Aftermath of the Promusicae Case: How to Strike the Balance?, Int. Jnl. of Law and Info. Technology, 2010, Volume 18, Issue 1, Pp. 50-71.

[46] T. Verbiest, Spindler G, et al., Study on the liability of Internet Intermediaries – General trends in Europe, Markt/2006/09/E, 12.11.2007, p.15; OECD, The Economic and Social Role of Internet Intermediaries, April 2010, p. 20; Barceló R. J. and Koelman, K., 'Intermediary Liability In The E-Commerce Directive: So Far So Good, But It's Not Enough', Computer Law & Security Report 2000, vol. 4, p. 231; Commission Communication to the European Parliament, The Council, The Economic and Social Committee and The Committee of Regions, A

III. Review of the E-Commerce Directive[47]

Despite the repeated criticism, the European Commission only started the process of reviewing the E-Commerce Directive in 2010.[48] The goal was to establish whether a revision was required. Following a stakeholder consultation, the European Commission released a report documenting the most often expressed complaints of the Directive in general, and the intermediary liability regime in particular.[49] The bulk of the latter concerned fragmentation and legal uncertainty.[50] Additionally, some specific problems regarding the hosting regime were described. A more thorough analysis of the identified issues was conducted in the Commission Staff Working Document on Online services.[51]

A. Criticism

The Commission Staff Working Document on Online Services expands on the problematic issues identified during the 2010 consultation. It mainly focused on the still pending questions with regard to legal uncertainty and fragmentation. Attention was also given to the specific issues of the hosting regime and the notice-and-takedown mechanism.

1. Legal Fragmentation

Legal fragmentation constitutes one of the greatest obstacles for the development of e-commerce in the EU. Despite the guarantees offered by the Directive, online intermediaries struggle with the fragmentation of rules that apply once they are aware of illegal content or activity on their websites.[52] It has been observed that the costs and risks arising from the coexistence of 28 national legal systems constrain innovation.[53] This factor discourages potential new players in the market and hampers development of online business.[54]

---

coherent framework for building trust in the Digital Single Market for e-commerce and online services {SEC(2011) 1640 final} http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:EN:PDF, p. 41;

[47] This section is based on: A. Kuczerawy, Intermediary Liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative, Computer Law and Security Review, Vol 31. Issue 1 2015, pages 46-56.

[48] Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC), http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm

[49] Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC), available at: http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf

[50] Ibid., p. 10 – 15.

[51] Commission Staff Working Document Online services, including e-commerce, in the Single Market, Brussels, 11.1.2012 SEC(2011) 1641 final *http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf*;

[52] Commission Communication to the European Parliament, The Council, The Economic and Social Committee and The Committee of Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services {SEC(2011) 1640 final} http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:EN:PDF, p. 14.

[53] Ibid. p. 6.

[54] Ibid. p. 14.

2. Legal Uncertainty

The most common criticism of the Directive refers to the unclear scope of the definitions of intermediaries.[55] As a result, it is often problematic to establish whether some services can benefit from the safe harbors offered by the ECD. This is particularly the case with 'new' types of services (e.g. video-sharing sites or social networking sites). Other criticisms mention the unclear position of search engines in the E-Commerce Directive. Opinions on the qualifications of this type of service differ across the EU.[56] Further, respondents to the consultation complained about the unclear conditions for exoneration.[57] Terms such as "expeditiously" or "actual knowledge" are defined in a way that leads to different interpretations in various countries by different stakeholders.[58] This makes the functioning of the internal EU market problematic for the providers of the online cross-border services, as well as for their users.

3. Notice and Takedown

Another issue is a lack of uniform rules implementing liability exemption procedures, such as a notice-and-takedown system, across the EU.[59] This is considered to be one of the major obstacles for intermediary service providers, as well as for victims of illegal content, to exercising their rights.[60] As mentioned above, the Directive left establishing specific procedures governing the removal or disabling of access to information to the discretion of the Member States. This possibility is delineated in art. 14.3, while art. 16 (and recital (40)) encourages self-regulation in this aspect. This however proved to be inefficient – only some countries introduced formal takedown procedures.[61] The procedures that were introduced are not harmonized with each other.[62] This leads to significant costs for all stakeholders in terms of both human and financial resources.[63]

The differences between the existing procedures can be quite substantial. Only a few countries foresaw any defense mechanism for the content provider ('counter-notice').[64] Very often a user has no means of defending what is a rightful use of the content. Moreover, the user might not

---

[55] Commission Staff Working Document Online services, including e-commerce, in the Single Market, Brussels, 11.1.2012 SEC(2011) 1641 final, p. 32 -39.

[56] Ibid., p. 26.

[57] Ibid., p. 43.

[58] Ibid., p. 32 -39.

[59] Ibid., p. 39 – 47.

[60] Ibid., p. 24 – 26.

[61] Van Eecke P., Truyens M., Legal analysis of a Single Market for the Information Society, New rules for a new age? a study commissioned by the European Commission's Information Society and Media Directorate-General, November 2009. Chapter 6: Liability of Online Intermediaries, p. 19.

[62] See more in the First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, at 13, COM (03) 0702, (November 21, 2003), available at: http://ec.europa.eu/internal_market/e-commerce/directive/index_en.htm#maincontentSec3

[63] Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC), p. 11.

[64] In particular Finland, Hungary, Lithuania, Spain and UK. See more in: First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on the Directive on Electronic Commerce, COM(2003) 702 final, Brussels, 21.11.2003.

even be aware that a third party objected to the use of the content, and which was, as a consequence, removed from the website in question. In most EU countries there is no requirement for hosting providers to inform content providers of any actions taken against their content.[65] These aspects of notice-and-take-down have been criticized on numerous occasions.[66]

These examples point out another weakness of the European intermediary liability regime. The E-Commerce Directive currently lacks any firm safeguards that would ensure the proper balance of the fundamental rights at stake.[67] No guidelines were advanced with regard to the implementation of takedown mechanisms implied in art. 14. Most EU countries did not foresee any procedural safeguards to ensure compatibility of notice-and-take-down regimes with the fundamental rights to freedom of expression, right to conduct business, due process, as well as the principle of proportionality.[68]

Hosting service providers can benefit from the liability exemption only if they 'act expeditiously' to remove or disable access to content upon obtaining notification about its illegal character. The decision to remove or disable has to be swift in order to exonerate the service provider from the potential liability. This often leads to 'over-compliance' with takedown requests. Specifically, it has been argued that this provision creates "an incentive to systematically take down material, without hearing from the party whose material is removed."[69] This is because any thorough assessment of the illicit character of content is not in the interest of the service provider. Moreover, the current legal situation is described as an "inappropriate transfer of juridical authority to the private sector."[70] These two factors may lead to private or corporate censorship.[71] Concern about a possible 'chilling effect' on freedom of expression in this process was expressed by a number of organizations, including the Council of Europe.[72] The

---

[65] T. Verbiest, Spindler G, et al., Study on the liability of Internet Intermediaries – General trends in Europe, Markt/2006/09/E, 12.11.2007

[66] Commission Staff Working Document Online services, including e-commerce, in the Single Market, Brussels, 11.1.2012 SEC(2011) 1641 final, p. 45; Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC), p. 12,available at: http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf

[67] Commission Staff Working Document Online services, including e-commerce, in the Single Market, Brussels, 11.1.2012 SEC(2011) 1641 final, p. 43 - 47.

[68] Horten M., The Copyright Enforcement Enigma – Internet Politics and the 'Telecoms Package', Palgrave Macmillan, 22 Nov 2011, p. 48-50;, T. Verbiest, Spindler G, et al., Study on the liability of Internet Intermediaries – General trends in Europe, Markt/2006/09/E, 12.11.2007.

[69] Barceló R. J. and Koelman, K., 'Intermediary Liability In The E-Commerce Directive: So Far So Good, But It's Not Enough', Computer Law & Security Report 2000, vol. 4, p. 231;

[70] Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC), p. 12

[71] Barceló R. J., On-line intermediary liability issues: comparing EU and US legal frameworks, E.I.P.R. 2000, 111; The Organization for Security and Co-Operation in Europe and Reporters Sans Frontiers, Joint declaration on guaranteeing media freedom on the Internet, 17-18.06.2005, available at: http://www.osce.org/fom/15657.

[72] Council of Europe (Council of Ministers), Declaration on freedom of communications on the Internet, 28.05.2003, available at: http://www.coe.int/t/informationsociety/documents/Freedom%20of%20communication%20on%20the%20Internet_en.pdf; Council of Europe, Human rights guidelines for Internet Service Providers – Developed by the Council of Europe in co-operation with the European Internet Service Providers Association (EuroISPA), July 2008, available at: http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)009_en.pdf, paras 16 and 24; T. Verbiest,

ongoing review of the Directive is aimed at tackling all identified issues, but it has proved to be very challenging.

B. Notice and Action Initiative

The 2010 consultation revealed that the majority of respondents did not see the need for a revision of the Directive at that stage. Many of them, however, expressed the need to clarify certain aspects of the Directive, particularly with regard to intermediaries' liability for third party content.

The European Commission also concluded that procedures aimed at eliminating illegal online content should lead to a quicker takedown, but at the same time should better respect fundamental rights (in particular freedom of expression) and should increase legal certainty for online intermediaries.[73] Based on these findings, the Commission decided to focus specifically on these aspects and direct its efforts to developing a new European framework for combating illicit online content.[74]

In January 2012, the European Commission announced a new initiative on 'Notice-and-Action' procedures.[75] The goal of this initiative is to set up a horizontal European framework for notice-and-action procedures, to combat illegality on the Internet, and to ensure the transparency, effectiveness, and proportionality of N&A procedures, as well as compliance with fundamental rights.[76] In order to combat illicit content more effectively, the Commission also announced a parallel revision of the Directive on the enforcement of intellectual property rights.[77]

Spindler G, et al., Study on the liability of Internet Intermediaries – General trends in Europe, Markt/2006/09/E, 12.11.2007, p.15; OECD, The Economic and Social Role of Internet Intermediaries, April 2010, pp. 9-14;

[73] European Commission on Notice and Action Procedures, http://ec.europa.eu/internal_market/e-commerce/notice-and-action/index_en.htm;

[74] Commission Communication to the European Parliament A coherent framework for building trust in the Digital Single Market for e-commerce and online services {SEC(2011) 1640 final} ;

[75] The main difference with Notice-and-Take Down is that in Notice-and-Action a broader range of actions against the content can be taken, providing a possibility for a tailored response (e.g. 'notice-and-notice' or 'notice-and-stay down'); '*The notice and action procedures are those followed by the intermediary Internet providers for the purpose of combating illegal content upon receipt of notification. The intermediary may, for example, take down illegal content, block it, or request that it be voluntarily taken down by the persons who posted it online*'. Commission Communication to the European Parliament, The Council, The Economic and Social Committee and The Committee of Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services {SEC(2011) 1640 final}, p. 13, ft. 49,
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:EN:PDF;

[76] *Ibid*., p.14;

[77] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights. OJ L 195, 2.6.2004. Commission Communication to the European Parliament A coherent framework for building trust in the Digital Single Market for e-commerce and online services {SEC(2011) 1640 final}, p. 15. See more on the Directive on the enforcement of intellectual property rights: http://ec.europa.eu/internal_market/iprenforcement/directive/index_en.htm; Action Plan on the enforcement of Intellectual Property Rights: http://ec.europa.eu/internal_market/iprenforcement/action-plan/index_en.htm#140701.

Following this announcement, the EC launched a new public consultation, this time dedicated entirely to N&A procedures.[78] In response, the EC received a great number of contributions from a wide range of stakeholders. They included businesses and business associations representing different types of intermediaries, as well as public authorities, lawyers, individual citizens, and members of the copyright industry and civil society. So far, the EC has not provided a formal response to the consultation and its results, even though a response was expected in 2013. As briefly summarized in the 2013 Action Plan, "the Commission services are working on an impact assessment of the notice-and-action procedures."[79]

According to Brussels insiders, the works are actually more intense that the official sources suggest. After the 2012 consultation, the EC was preparing a proposal for a new Notice-and-Action Directive. Such a Directive would address the problem of online intermediaries' uncertainty without the need to amend the whole E-Commerce Directive. The proposal, however, has not yet officially surfaced.[80] It seems however that the works have currently slowed down. Several commentators suggested that, in the light of the 2014 European elections, the proposal was (at least temporarily) withdrawn due to a heavy industry lobbying effort and general sensitivity to the issue.[81] There are indications that the topic has not been abandoned and it will return onto the EU policy agenda after the 2014 European elections.[82]

IV. Situation of Search Engines

A. Relevance of Search Engines / Information Location Tool Services

Search engines are a type of selection intermediary, also called information location tool services or referencing services. Their role is to map, order, select, validate, and valuate online information. By doing this, they can help users to navigate the Web with its abundance of information. By providing a way to overcome 'information overload,' search engines guarantee the free flow of information and deliver a crucial service to society. It could be said that by providing access to information and diverse opinions they participate in ensuring freedom of expression, as delineated in art. 10 of the European Convention of Human Rights.[83]

---

[78] A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries, http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-Internet_en.htm

[79] Commission Staff Working Document E-commerce Action plan 2012-2015 - State of play 2013, Brussels, 23.4.2013 SWD(2013) 153 final, p. 19, available at: http://ec.europa.eu/internal_market/e-commerce/docs/communications/130423_report-ecommerce-action-plan_en.pdf

[80] See: Open Letter to Commissioner Barnier, https://ameliaandersdotter.eu/sites/default/files/letter_commissioner_barnier_notice_and_takedown.pdf .

[81] Monica Horten, 2013, Notice and action directive to be blocked as EU backs down, 28 July 2013. Available at: http://www.iptegrity.com/index.php/ipred/893-notice-and-action-directive-to-be-blocked-as-eu-backs-down.

[82] Recently, Commissioner Barnier indicated that the works on the N&A initiative shall continue when speaking to the European Parliament. See more at: Monica Horten, 2014, Notice of Action! Barnier to resurrect take-down directive, in Iptegrity.com 6 February 2014. Available at: http://www.iptegrity.com/index.php/ipred/945-notice-of-action-eu-commission-to-revive-take-down-directive;

[83] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No. 005, 04.11.1950, Rome, retrieved from http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm. See also

Information location tool services, or search engines, are covered by the definition of the Information Society Service from the E-Commerce Directive. In Recital 18 it is stated that:

> "[I]nformation society services are not solely restricted to services giving rise to online contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data…"[84]

However, this type of service is not covered by any of the three definitions of the services described in Section 4 of the E-Commerce Directive. They are, strictly speaking, neither a mere-conduit service, nor caching or hosting service. This would mean that the intermediary liability regime of art. 12-15 ECD does not cover, at least nominally, search engines (or hyperlinks). The Directive, therefore, leaves this issue unattended.[85] Only in the Final Provisions of the Directive is the problem mentioned, as it appears on the list of topics that should be analyzed in future, during the re-examination of the document. In Article 21 the Directive specifies that: "In examining the need for an adaptation of this Directive, the report shall in particular analyze the need for proposals concerning the liability of providers of hyperlinks and location tool services…"[86]

This means that, until now, the E-Commerce Directive had not specifically addressed the legal situation of search engines with regard to liability for third party content. As can be seen in numerous examples of cases at both the national and the EU level, this approach creates a certain amount of confusion.[87]

Some of the most active search engines in Europe try to deal with this obstacle (at least partially) through different, and possibly combined, strategies. In some cases, search engine providers look for a solution by providing localized versions of their services.[88] This practice is especially common in the case of highly sensitive content, such as Nazi glorification – prohibited by some European countries. In the majority of the cases, non-European search engines design their policies in accordance with the national laws of their countries of origin. Given the fact that most of them are based in the US, this has led to a *de facto* application of the US regime, especially

---

Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, (Adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies).

[84] Directive 2000/31, Recital (18).

[85] Van Eecke P., Truyens M., Legal analysis of a Single Market for the Information Society, New rules for a new age? a study commissioned by the European Commission's Information Society and Media Directorate-General, November 2009. Chapter 6: Liability of Online Intermediaries, p. 25.

[86] Directive 2000/31/EC, art. 21(2).

[87] Spain: Miguel v. Google Inc., Spanish Supreme Court [STS (Civil Chamber) of 4 March 2013 no. 144/2013]; Spanish Supreme Court, Civil Chamber, ruling of 9 December 2009, no. 773/2009; Spanish Supreme Court, Civil Chamber, ruling of 4 March 2013 no. 144/2013; UK: R v Rock and Overton, Crown Court, Gloucester, 06.02.2010, ref. no. T20097013; Belgium, Brussels Court of First Instance, 15.02.2007, ref. no. 7964; Germany: Deutscher Bundesgerichtshof (BGH), 29.04.2010, ref. no. I ZR 69/08;

[88] W. Seltzer, "The Politics of Internet Control and Delegated Censorship", American Society of International Law, April 10, 2008, p. 3, accessible at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1496056.

with regard to copyright infringements (cfr. Section 230, DMCA).[89] As a result, the search engines governance debate in Europe is strongly influenced by the US approach (which also became clear in the *Google Spain* Case).[90]

B. Search Engines Regulation Across the EU

The E-Commerce Directive declined to address the situation of search engines with regard to third party's content. This issue was left entirely to the discretion of the Member States. Some countries have taken advantage of this opportunity, according to the EC's first report on the application of the E-Commerce Directive.[91] The result is a variety of approaches across the EU.

Some countries extended the legislation transposing the E-Commerce Directive in order to cover search engines (and hyperlinks). This result was achieved mostly by adding an additional provision that targets these types of services. Among those Member States, two trends arise.

In Austria and Liechtenstein, for example, search engine services were classified as providers of 'access services.' As a result, they were provided with a liability exemption similar to that of the providers of mere conduit services. The argument behind this classification was that "search engines generally do not edit the content they show in the results, are not the source of the information they link to, and are not in the position to remove it from the Web."[92]

Other Member States, such as Hungary[93], Portugal,[94] and Spain[95] have opted for the hosting model for both search engines and hyperlinks. This means that providers of these services are

---

[89] The most popular search engines like Google, Bing and Yahoo! are US based companies. For Google's policy see the Transparency Report FAQ: "It is our policy to respond to clear and specific notices of alleged copyright infringement. The form of notice we specify in our web form is consistent with the DMCA and provides a simple and efficient mechanism for copyright owners from countries around the world." http://www.google.com/transparencyreport/removals/copyright/faq/#other_copyright_laws

[90] J. Van Hoboken, Search engine freedom. On the implications of the right to freedom of expression for the legal governance of Web search engines, Academisch Proefschrift ter verkrijging van de graad van doctor aan de Universiteit van Amsterdam, defended on 23 March 2012, p. 70.

[91] First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, at 13, COM (03) 0702, (November 21, 2003), available at: http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2003/0702/COM_COM(2003)0702_EN.pdf.

[92] See footnote 30 in: Van Hoboken J., Legal Space for Innovative Ordering: on the need to update selection intermediary liability in the EU, International Journal of Communications Law & Policy, Issue 13, Winter 2009

[93] See 2001. évi CVIII Törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről [Act CVIII of 2001 on Electronic Commercial Services and Certain Legal Aspects of Information Society Services] (promulgated 24 Dec., 2001), MAGYAR KÖZLÖNY [HUNGARIAN GAZETTE] 2001/153, translated in http://www.nhh.hu/dokumentum.php?cid=11961.

[94] See Decreto- Lei n.º 7/2004, de 7 de Janeiro, que transpõe para a ordem jurídica nacional a Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno; Decreto-Lei 62/2009; Official Journal: Diaro da Republica I, number: 48, Publication date: 10/03/2009, p. 01602-01602 (MNE(2009)51108) http://www.cnpd.pt/bin/legis/nacional/DL62-2009-SPAM.pdf

[95] See art. 17 of Law 34/2002 on Information Society Services and Electronic Commerce (Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electronicó) of 12 July 2002 (B.O.E. 2002, 166). For a short a discussion see R. Julia- Barceló, 'Spanish Implementation of the E-Commerce Directive. Main features of the

exempted from liability if they do not have knowledge of the illegal nature of the information they are linking to. They must also act expeditiously in case they obtain such knowledge, for example upon a notification from an individual, administrative body, or a court.

The third group of the EU countries left this issue unregulated, choosing instead to apply the general rules of existing law. The best example here is the U.K., which is waiting for the European Commission to deal with this issue.[96] A similar situation can be found in Germany and the Netherlands, where the general rules of law, particularly tort law, are applied.[97] Very often, this results in complex rulings of the respective courts on the subject matter.[98]

The situation of search engines with regard to third party content is therefore far from harmonized at the EU level. The level of complexity of the underlying issues and the varying national approaches create a situation of legal uncertainty that is problematic for the providers of these services. This can be illustrated with the variety of decisions of different European courts with regard to the legal situation of the biggest player on the European search market: Google.[99]

This climate of legal uncertainty and fragmentation could also pose considerable difficulties for new, smaller market players that very often cannot afford elaborate legal services to determine the liabilities of their particular business models.[100] This could be considered an obstacle to entering the field and, as a result, could hamper innovation and competition in the European market.[101] It has already been observed that the major multinational selection intermediaries tend to choose compliance with the US law, which provides them with liability exemptions necessary to ensure their lawful operation.[102] Applicability of the EU legislation to the US based services,

---

Implementation of the Ecommerce directive in Spain', *Computer und Recht International* 2002, p. 112. See also Spanish Data Protection Agency (AEPD), Statement on Internet Search Engines, p. 2 et seq., available at: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/statement_aepd_search_engines_/Statement_AEPD_Search_Engines_en.pdf.

[96] DTI Consultation Document on the Electronic Commerce Directive: The Liability of Hyperlinkers, Location Tool Services and Content Aggregators - Government Response and Summary of Responses 6 (December 2006), available at http://www.berr.gov.uk/files/file35905.pdf.

[97] See Sieber U., Liesching M., Die Verantwortlichkeit der Suchmaschinenbetreiber nach dem Telemediengesetz [The Liability of Search Engine Operators after the Telemedia Act], MULTIMEDIA UND RECHT [MMR], Issue 8/2007; Peter Ruess, 'Just Google it?' – Neuigkeiten und Gedanken zur Haftung der Suchmaschinenanbieter für Markenverletzungen in Deutschland und den USA ['Just Google it?' – Novelties and Thoughts on the Liability of Search Engine Operators for Trademark Infringement in Germany and the USA], 2007 GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT 198 – 203.

[98] Germany: Bundesgerichtshof [BGH][Federal Court of Justice] Jul 17, 2003, I ZR 259/00; Oberlandesgericht [OLG] Hamburg [Court of Appeals Hamburg], February 20, 2007, AZ. 7 U 126/06; Landesgericht [LG] Berlin [Trial Court Berlin], February 22, 2005, AZ 27 O 45/05; Netherlands: Hof Amsterdam, 15 June 2006, Stichting BREIN vs. Techno Design Internet Programming BV, case LJ number AX7579'.

[99] E.g. European Court of Justice, Joined Cases C-236/08 to C-238/08, 23 March 2010 (Google France and Google v. Louis Vuitton Malletier a.o.); Court of Appeal, Case no. 08/13423, 26 January 2011 (Socie´te´ des Auteurs des Arts visuels et de l'Image fixe (SAIF) v Google France/Google inc.); The Court of Appeal of Brussels, Case no. 2007/AR/1730, 5 May 2011 (Copiepresse v. Google); Court of Milan, Case no. 1972/2010, 24 February 2010.

[100] Van Hoboken J., Legal Space for Innovative Ordering: on the need to update selection intermediary liability in the EU, International Journal of Communications Law & Policy, Issue 13, Winter 2009.

[101] Ibid.

[102] J. Grimmelmann, The Structure of Search Engine Law, 93 IOWA L. REV. 1 (2007); U. Gasser, Regulating Search Engines: Taking Stock and Looking Ahead, 8 YALE J. L. & TECH. 124 (2006).

including search engines, has been debated extensively over the last few years.[103] This issue has been addressed in a recent high-profile case at the CJEU Google Spain, which will be presented below.

V. Google Spain Case

The so-called *Google Spain* Case (recently before the Court of Justice of the European Union (C-131/12)) constitutes an excellent example of the issues mentioned in the previous pages.[104] The case raises crucial questions lying at the intersection of the legal regimes concerning intermediary liability, freedom of expression, privacy, and data protection.[105] Interestingly enough, the Court's decision hinged entirely upon the European data protection framework. In other words, the Court barely mentioned the right to freedom of expression and made no reference whatsoever to intermediary liability exemptions.[106] The following section will give a brief overview of the main issues in this case when looked at from an intermediary liability angle. But before that, we briefly recall the main facts of the case.

A. The Ruling[107]

1. Facts

In the late 1990's a Spanish citizen was subjected to insolvency proceedings, which in turn resulted in a public auction of some of his property. Information about this public auction was published in a local newspaper (*LaVanguardia*), in accordance with an order issued by the Spanish Ministry of Labor and Social Affairs.[108] By 1998, all debts were successfully settled.

In 2009, the Spanish citizen discovered references to the above-mentioned *LaVanguardia* article when entering his name into Google's search engine. Disturbed, he asked the newspaper to remove the content in question. This request was denied, as the newspaper had a legal obligation

---

[103] Article 29 Data Protection Working Party, 'Opinion 8/2010 on applicable law', WP 179, 16 December 2010, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf; L. Moerel, 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?', International Data Privacy Law 2011, Vol. 1, No. 1, p. 34-35; C. Kuner, F.H. Cate, C. Millard and D.J.B. Svantesson, 'The extraterritoriality of data privacy laws – an explosive issue yet to detonate', International Data Privacy Law 2013, Vol. 3, No. 3, p. 147-148; A. Kuczerawy, Facebook and its EU users - applicability of the EU data protection law to US based SNS, in M. Bezzi et al. (Eds.): Privacy and Identity, IFIP AICT 320, 2010, pp. 75–85.

[104] Court of Justice of the European Union, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12, 13 May 2014.

[105] For an elaborate discussion on all theses issues, see: Alsenoy, Van, Brendan, Aleksandra Kuczerawy, and Jef Ausloos. *Search Engines after "Google Spain": Internet@Liberty or Privacy@Peril?*. ICRI Research Paper. Leuven, Belgium: ICRI, September 6, 2013. http://papers.ssrn.com/abstract=2321494.

[106] This is in sharp contrast to the Advocate General's Opinion of June 2013. REFERENCE

[107] This section is largely based on a similar section in another paper the authors co-wrote: Van Alsenoy, Brendan, Aleksandra Kuczerawy, and Jef Ausloos. Search Engines after "Google Spain": Internet@Liberty or Privacy@Peril? ICRI Research Paper. Leuven, Belgium: ICRI, September 6, 2013. http://papers.ssrn.com/abstract=2321494, 6.

[108] Audiencia Nacional. Sala de lo Contencioso, *Google Spain SL y Google Inc., S.L. c. Agencia de Protección de Datos,* paragraph 1.2, available at http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=6292979&links=%22725/2010%22&optimize=20120305&publicinterface=true

to publish this information. Unsuccessful vis-à-vis the newspaper itself, the individual then requested Google's Spanish subsidiary (hereafter: 'Google Es.') to stop including this article in search results when someone enters his name as a search term.[109] Google Es. referred this request to Google Inc., arguing that this is the entity responsible for the development of search results.

In March of 2010, the individual asked the Spanish Data Protection Authority (*Agencia Española de Protección de Datos*, AEPD) to issue an administrative decision which would (a) order *LaVanguardia* to eliminate or modify the publication so his personal data would no longer appear in search results; and (b) order Google to stop referring to the contentious publication in its search results.[110] In July of the same year, the AEPD ordered Google Es. and Google Inc. to take "*all reasonable steps to remove the disputed personal data from its index and preclude further access*."[111] The request against *La Vanguardia* was denied, because – according to the AEPD – the newspaper still had a legitimate reason to process the data at issue.[112] One year later, Google launched an appeal against the AEPD's decision before the Spanish National Court (*Audiencia Nacional)* in Madrid. In March 2012, this court referred the case to the Court of Justice of the European Union (CJEU) for a preliminary ruling.[113]

2. Decision

The Court of Justice issued its ruling on May 13th 2014. To the surprise of many, the decision entirely countered the Advocate General's Opinion of June 2013.[114] Put briefly, the Court decided that Google – and 'search engine operators' more broadly – do fall within the scope of application of European data protection law. After all, the Court declared, by (autonomously) retrieving, recording, and organizing personal data from third party websites, search engines can be considered 'data controllers' within the meaning of the data protection directive (95/46).[115] The Court also resolutely decided that Google falls within the Directive's *territorial* scope of application.[116] Following this first category of questions (regarding the scope of application of

---

[109] Ibid, paragraph 1.3.

[110] *Ibid*, paragraph 2.1

[111] *Ibid*, paragraph 2.3.

[112] i.e. order issued by the Spanish Ministry of Labour and Social Affairs *Ibid*, paragraph 6.2.

[113] At the risk of generalizing too much, the request for a preliminary ruling contained two categories of questions: (a) the scope of application of European data protection law; and (b) the existence of a right to be forgotten/erasure vis-à-vis search engines directly.

[114] In this non-binding, advisory document to the Court, the Advocate General argued that search engines do not fall within the scope of application of the data protection framework with regard to the content they refer to. Moreover, he claimed that the current EU data protection directive does not provide for a general 'right to be forgotten' vis-a-vis search engines. Opinion of Advocate General Jääskinen, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González,* Case C□131/12, 25 June 2013, in particular paras. 100; 108.

[115] For the Court's reasoning, see Ruling paras. 21-32 on the Material Scope Determination ('processing' and 'personal data') and paras.32-41 on the Personal Scope Determination ('data controller'). For a detailed academic analysis, see: Alsenoy, Van, Brendan, Aleksandra Kuczerawy, and Jef Ausloos. *Search Engines after "Google Spain": Internet@Liberty or Privacy@Peril?* ICRI Research Paper. Leuven, Belgium: ICRI, September 6, 2013. http://papers.ssrn.com/abstract=2321494, 9-19.

[116] See Paras.42-60 of the Ruling.
From a practical perspective, this means non-EU intermediaries (or Internet service providers more broadly) will not be able to escape the territorial reach of the data protection framework when they are processing EU citizens' personal data and have an establishment in the Union.

European data protection law), the Court dealt with the more controversial questions regarding the so-called 'Right to be Forgotten'. In short, it decided that data subjects can indeed ask search engines to remove a reference to a webpage when their name is used as a search term.[117] The lawfulness of the source material is not a condition,[118] nor does the data subject have to prove harm.[119] The Court did specify, however, that the right to erasure is not absolute, and a balance of rights and interests needs to be made.[120] These rights and interests include, on the one hand, the economic interests of the search engine operator, as well as the legitimate interests of Internet users in accessing information and, on the other hand, data subject's rights. According to the Court of Justice, the search engine's economic interests alone cannot be a justification to interfere with the data subject's rights. With regard to the balancing of fundamental rights and interests of Internet users versus those of the data subject, the Court did state that the latter override all others by default.[121] In other words, the burden of proof seems to be on the search engine to establish that the interests/rights of its users weigh more than those of the data subject. The Court did provide some guidance on what criteria might influence the balancing exercise *in casu*: nature or sensitivity of the information; public interest; role of data subject in public life; time elapsed; etc.[122] In any situation, it is important to emphasize that the data subject will still have to fulfill the conditions for exercising his/her right to object/erase[123] and the search engine is only subject to data protection rules "within the framework of its responsibilities, powers, and capabilities."[124]

B. Particularities

Even though entirely ruled under the data protection framework, the Google Spain (or 'Right to be Forgotten') case[125] bears a lot of resemblance to the notice-and-takedown procedures that people are more familiar with under the intermediary liability regime (*supra*). After all, an individual – with certain rights vis-à-vis the information – demands an entity that is not at the

---

Following the ruling, Google has clarified that it will only comply with potential erasure requests when the search queries originate in the EU. Put differently, the takedowns will not be implemented globally (see: Sam Schechner, "Google Starts Removing Search Results under Europe's 'Right to Be Forgotten,'" *Wall Street Journal*, June 26, 2014, sec. Technology, http://online.wsj.com/articles/google-starts-removing-search-results-under-europes-right-to-be-forgotten-1403774023. This article also explains at least one regulator has expressed displeasure in this regard). Whether or not Member-States will deem this an appropriate reaction still has to be seen.

[117] Such a right would be based on the rights to object (14) and to erasure (12(b)) in the Data Protection Directive.

[118] Paragraph 88; 93-94.

[119] Paragraph 96; 99.

[120] Paragraphs 74 *et seq*.

[121] Paragraph 81; 97.

[122] Paragraph 81; 93.

[123] In order to exercise one's right to object, the data subject will have to put forward 'compelling legitimate grounds relating to his/her particular situation to the processing of data relating to him/her' (article 14 Directive 95/46). The right to erasure can be exercised when the processing in question 'does not comply with the provisions of [the] Directive, in particular because of the incomplete or inaccurate nature of the data' (article 12(b)).

[124] Paragraph 83.

[125] For a comprehensive overview of the possibility to request the removal of (links to) personal data by search engines, see: Van Alsenoy , Brendan, Aleksandra Kuczerawy, and Jef Ausloos. *Search Engines after "Google Spain": Internet@Liberty or Privacy@Peril?* ICRI Research Paper. Leuven, Belgium: ICRI, September 6, 2013. http://papers.ssrn.com/abstract=2321494.

source of the information, to remove it. Nevertheless, there are some important questions that distinguish this particular case from traditional N&T procedures.

1. Notification

As has been described *supra*, search engines are not explicitly included in the intermediary liability exemption regime in the E-Commerce Directive.

However, Spanish law explicitly provides for a search engine liability exemption, similar to that for hosting providers.[126] In the *Google Spain* Case, however, the Court put emphasis on the search engine's own activities vis-à-vis the (personal) data and not the activities of the original publisher. The latter, after all, were legal.

Once notified of a certain processing activity (i.e. the referral to a certain website upon searching for someone's name), it was argued, Google cannot deny its responsibility with regard to that processing. It is therefore worth highlighting that in *Google Spain,* the rights holder (i.e. the data subject) *did* notify the search engine. When the company did not react, the individual eventually obtained a court order to have the respective information taken down. Therefore, when looked at from an intermediary liability perspective, Google would still have had to remove the information upon notification (cfr. the hosting regime). *In casu*, they did not even remove it after receiving a court order (cfr. mere conduit regime, where information has to be removed following such an order).[127]

2. Taking Down Legitimate Information?

One of the elements making the *Google Spain* Case so interesting and controversial is the fact that the underlying information – which is referred to by Google – is published lawfully. In other words, the information at its source is legitimate and the original publisher does not have an obligation to take it down.[128] It is in this context the analogy with the notice-and-takedown regime falls apart. The exemption regime under the E-Commerce Directive focuses on the (illegal) nature of the content or the activities of the originator. The Data Protection Directive, on the other hand, focuses on the activities of the controller itself (*in casu* the search engine), regardless of those of the entity at the source of the information. This approach goes back to the

---

[126] *Supra*, Section 3.2; Recently, Google was explicitly ruled not to have actual knowledge in a case where a victim of defamation had issued a takedown request and even obtained a judgment declaring the original content to be illegal. See more: C. A. Rigaudias, "Miguel v. Google Inc. Spanish Supreme Court [STS (Civil Chamber) of 4 March 2013 no. 144/2013] – "The recent judgment of the Spanish Supreme Court addressed the liability of intermediary information services providers for defamatory content and sheds light on the so-called 'right to be forgotten' case being heard by the ECJ", E-Commerce Law Reports - volume 13 issue 04, p. 11

[127] Clearly, it was a deliberate and strategic decision on Google's part not to comply with this specific injunction. Besides wanting to obtain a more definitive and authoritative answer on whether or not these kind of erasure requests should be possible in the first place, Google was probably interested in being elucidated on who will bear the costs of compliance. Do search engines (exclusively) bear the burden of assessing removal requests? Or can they just defer to the authorities (DPA or Court) to make the appropriate balance? The CJEU seems to suggest a middle-way, in which search engines can be asked to make a balance, but can easily defer the requester to the relevant national authority in more problematic cases (without risking liability).

[128] In this particular case, the original source (*LaVanguardia*) even had an explicit obligation to publish the information.

Court of Justice's *Lindqvist*[129] and *Satamedia*[130] cases. In these cases, the Court emphasized that personal data that has been published is still protected by data protection law. Each use of the relevant personal data should hence be assessed against data protection law separately. To put this differently, the data protection framework – and right to erasure in particular – starts from a different paradigm than the liability exemptions in the E-Commerce Directive. The latter is hinged upon traditional tort law principles where an individual is subject to (potential) harm caused by the publication of certain information. Data protection simply puts certain responsibilities on the shoulders of whoever *processes* personal data. In order to exercise one's rights under the data protection framework, it is not necessary to demonstrate (potential) harm.[131]

3. Autonomy

Contrary to the intermediaries mentioned in Section 4 of the E-Commerce Directive (e.g. caching, mere conduit and hosting providers), search engines do not remain purely passive with regard to the information they facilitate access to.[132] In fact, they do a great deal with this data independent from gathering it from its source.[133] Based on their algorithmic analysis of the information, they refer to certain web pages when entering a particular search term/phrase. A strong argument can be made that search engines bear responsibility for this specific activity. After all, it determines – entirely autonomously – how and why the information is presented in a certain way. But, one could counter-argue that search engines only offer a tool to their users and should not be held responsible for the queries these users make.

In any situation, it is hard to deny the importance of search engines in giving visibility/publicity to the information they refer to. In *Google Spain*, the Court emphasized that search results constitute "a structured overview of the information [...] that can be found on the Internet [...] and which, without the search engine, could not have been interconnected or could have been only with great difficulty – and thereby to establish a more or less detailed profile...".[134] While this is – of course – one of the main reasons people use search engines in the first place, it is also the reason why a search engine has such a potentially important impact on users' perception of the search term. In other words, the harm or impact on the individual might not have occurred (to the same extent) if the information had not been accessible through search engines.[135] Put briefly,

---

[129] *Court of Justice of the European Union , Bodil Lindqvist, C-101/01, 6 November 2003,*

[130] *Court of Justice of the European Union, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, C□73/07, 16 December 2008*

[131] Article 23 of the Directive does provide for the possibility to obtain damages in case one is actually harmed.

[132] Intermediary liability exemptions are based on the premise that the 'sole purpose' of their activities is to make "the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored." (recital 42 of the E-Commerce Directive).

[133] For a comprehensive overview, see: Van Alsenoy *et al*., 11 *et seq*.This is probably also one of the reasons why search engines are not explicitly included in the E-Commerce Directive's exemption regime in the first place. The legislator specifically introduced an article spurring the European Commission to analyse "the need for proposals concerning the liability of providers of hyperlinks and location tool services." (article 21.2).In the *Google Spain* Case, the Court of Justice emphasized the distinction between the search engine's and the original publisher's activities at several occasions: Paragraph 80; 84-85; 86-87.

[134] Paragraph 80.

[135] This line of arguments was already put forward by the Spanish DPA in a Statement dating back from December 2007. Spanish Data Protection Agency, *Statement on Internet Search Engines* (Madrid, Spain, December 1, 2007),

one could draw a direct causal relationship between the search engine's activities and the impact on the individual. Hence, it is not surprising to see the Council of the EU also emphasize that the required balancing exercise differs depending on whether it relates to taking down the source or a search link.[136]

The above is well-illustrated by two Australian cases involving Yahoo![137] and Google.[138] In these (defamation) cases, the plaintiff successfully established that the search engines' result pages caused him reputational harm. The links, snippets, and photos that were shown when searching for the plaintiff's name – and which were all legal/legitimate on their own – gave the impression Mr. Trkulja was a criminal.[139] In the same vein, several European courts have recognized that – under certain circumstances – Google's 'auto-complete' functionality can cause harm to the relevant individual. For example, a German Federal Court recently ruled that Google should remove offensive word-combinations upon notification (*in casu* 'scientology').[140] In a comparable and ongoing case, Bettina Wulff (the former First Lady of Germany) has demanded that Google cease auto-completion with words such as 'escort' and 'red light district' when entering her name.[141] Similarly, an Italian court has ruled Google to be responsible for the auto-complete terms '*truffatore*' (con man, swindler) and '*truffa*' (scam, fraud).[142] Other cases against Google's auto-complete functionality were introduced by companies, seeing their name being associated with terms such as 'receivership'[143]; 'crook'[144]; 'scam'[145]; etc.

9–10. The DPA stated *inter alia* that "*Although the initial incorporation of this personal information on the web 'may be legitimate at source, its universal and secular conservation on the Internet may be disproportionate.' People must have at their disposal reaction instruments in order to avoid, on their own initiative, to be subject to a global exhibition*."

[136] Council of the European Union - Working Group on Information Exchange and Data Protection (DAPIX). "Note on the Proposal for a General Data Protection Regulation - the Right to Be Forgotten and the Google Judgment," July 3, 2014. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011289%202014%20INIT, 5-6.

[137] Trkulja v Yahoo! Inc LLC & Anor (VSC 2012).

[138] Trkulja v Google Inc LLC & Anor (No 5) (VSC 2012).

[139] More specifically, when looking for the plaintiff's name, search engine users were presented with pictures of criminals with the plaintiff's name underneath. The results pages also contained a link to an article titled 'Shooting probe urged ...' aside a big picture of the plaintiff and underneath the heading 'Melbourne Crime'.

[140] BGH, judgment of 14 May 2013, ref. VI ZR 269/12, available at http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2013&nr=64071&pos=0&anz=86. Also see: EDRi. "Germany: Google Must Remove Autocomplete Harmful Searches If Notified," May 22, 2013. edri.org/edrigram/number11.10/autocomplete-harmful-searches-google-germany; "German Federal Court Raps Google on the Knuckles over Autocomplete Function | Technology | DW.DE | 15.05.2013," *DW.DE*, accessed June 25, 2013, http://www.dw.de/german-federal-court-raps-google-on-the-knuckles-over-autocomplete-function/a-16813363.

[141] "Bettina Wulff Will Weiter Gegen Google Vorgehen," *Welt Online*, May 20, 2013, sec. Wirtschaft, http://www.welt.de/wirtschaft/article116355211/Bettina-Wulff-will-weiter-gegen-Google-vorgehen.html; "German Federal Court Raps Google on the Knuckles over Autocomplete Function | Technology | DW.DE | 15.05.2013."

[142] EDRi, "Italian Court Found Google Responsible For Search Suggestions To Users," April 20, 2011, http://www.edri.org/edrigram/number9.8/italian-case-google-suggest.

[143] In 2011, an Irish hotel sued Google over the search term suggestion 'receivership' ("the legal state of having forfeited control of a business or estate to a receiver to allow for the attempted recovery of a debt"). The case was later dropped by the Hotel for unclear reasons. See: Rob Young, "Irish Hotel Drops Autocomplete Defamation Case Against Google," *Search Engine Watch*, November 25, 2011, http://searchenginewatch.com/article/2127329/Irish-Hotel-Drops-Autocomplete-Defamation-Case-Against-Google.

In any situation, the above clearly illustrates the difficulties of categorizing search engines or even defining the nature of their activities. It is clear that, on the one hand, they do perform autonomous and independent activities on the information, while on the other hand acting as a mere intermediary facilitating access to third party content. But it is much less clear whether this conceptual distinction can – or even should – be translated into practice.

C. Aftermath

Only two weeks after the CJEU's decision, Google had already put in place an online form, allowing individuals to request the removal of links from the results that were produced by a search of their name.[146] At the same time, the search engine company also announced it would create a hand-picked team of experts.[147] This 'advisory council' will help them define a strategy on how to deal with the multitude of requests that they receive, and includes academics, policymakers, business people, and journalists.[148] More recently, Google also invited the public at large to give them feedback on how to implement the ruling.[149] Some national data protection authorities have issued official reactions to the ruling already[150] and the Article 29 Working Party[151] has already had an internal meeting on the Court's ruling,[152] and sat together with several search engines at the end of July.[153]

---

[144] In France, a Court of Appeals confirmed an earlier decision, requiring Google to remove the auto-suggestion, pay €50.000 in damages and publish the decision on its homepage. See: "Google Suggest Condamné En Appel Pour Injure - LeMonde.fr," accessed December 29, 2011, http://www.lemonde.fr/technologies/article/2011/12/28/google-suggest-condamne-en-appel-pour-injure_1623293_651865.html.

[145] Marc Rees, "Google Condamné Pour Avoir Suggéré La Requête," January 6, 2010, pcinpact.com/news/54815-google-suggest-arnaque-requete-moteur.htm.

[146] https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=en

[147] Alistair Barr and Rolfe Winkler, "Google Offers 'Right to Be Forgotten' Form in Europe," *Wall Street Journal*, May 30, 2014, http://online.wsj.com/articles/google-committee-of-experts-to-deal-with-right-to-be-forgotten-1401426748.

[148] See: https://www.google.com/advisorycouncil/

[149] https://www.google.com/advisorycouncil/

[150] For example: The Spanish DPA being generally positive but emphasizing the need for a thorough impact assessment (AEPD, *Press Release - The Court of Justice of the European Union supports the thesis of the Spanish DPA on search engines and the right to be forgotten online*, 13 May 2014, http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/may_14/Press_release_EU_Court_judgement_right_to_be_forgotten1.pdf); the UK's information Commissioner declared there is an important role to be played by national regulators (David Smith (Deputy Commissioner and Director of Data Protection, ICO), *Four things we learned from the EU Google judgment*, 20 May 2014, http://iconewsblog.wordpress.com/2014/05/20/four-things-weve-learned-from-the-eu-google-judgment.).

[151] Umbrella organization including the data protection authorities from all EU member states. See: http://ec.europa.eu/justice/data-protection/article-29/

[152] Article 29 Data Protection Working Party, *Press Release*, 23 May 2014, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140523_wp29_press_release_ecj_google.pdf

[153] http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140717_wp29_press_release_meeting_with_search_engines.pdf
For a complete list of the concrete questions the Working Party asked the search engines, see: Article 29 Working Party, "Press Release: European DPAs Meet with Search Engines on the 'right to Be Forgotten,'" July 25, 2014, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140725_wp29_press_release_right_to_be_forgotten.pdf.

Twenty-four hours after putting the form online where individuals can ask Google to remove certain links, the search engine already reported receiving over 12,000 requests. This number climbed to 41,000 by early June[154] and over 70,000 one month after that.[155][156] Most requests emanated from France, than Germany, Great Britain, and Spain.[157] Google declared to regulators that it approved over 50% of the requests, asked for more information in about 15%, and rejected over 30%.

At first, the search engine intended to notify its users when their search query would have been the subject of an erasure request under the data protection framework (similarly to what it does with regard to takedowns in the context of copyright).[158] Instead, however, Google now puts a disclaimer on the bottom of every search it identifies as a 'name search', stating, "*Some results may have been removed under data protection law in Europe,*" with a link to more information on the CJEU case. It seems, though, that Google will try to notify the relevant source in certain cases. This was clearly illustrated when the Guardian[159] and BBC[160] published reports that some of their articles on corrupt politicians, dodgy bankers, and pedophiles had been de-indexed by Google.[161] Finally, it should be said that all of the above only occurs within the context of the

---

[154] Jennifer Baker, "Google Has Received over 41,000 Requests to 'Forget' Personal Information," Tech Blog, *IT World*, (June 4, 2014), http://www.itworld.com/networking/421740/google-has-received-over-41000-requests-forget-personal-information.

[155] Op-Ed by Google's Chief Legal Officer D. Drummond: http://googleblog.blogspot.be/2014/07/searching-for-right-balance.html. By the end of July, Google reported to have received over 91.000 requests. See: David Lee, "Google Quizzed over Deleted Links," *BBC News*, July 24, 2014, www.bbc.com/news/technology-28458194.

[156] These numbers seem to indicate a progressive decline of requests. Anecdotally, it is worth mentioning that Bing (Microsoft's search engine) only received around 20 requests the day after Google released its erasure-form (see:Mark Scott, "Microsoft Taking Steps to Comply With the Right to Be Forgotten," *New York Times*, July 9, 2014, sec. Bits Blog, http://bits.blogs.nytimes.com/2014/07/09/microsoft-to-wade-into-complying-with-the-right-to-be-forgotten/.)

[157] Lee, "Google Quizzed over Deleted Links."

[158] Josh Halliday, "Google Search Results May Indicate 'Right to Be Forgotten' Censorship," *The Guardian*, June 8, 2014, sec. Technology, http://www.theguardian.com/technology/2014/jun/08/google-search-results-indicate-right-to-be-forgotten-censorship.

[159] James Ball, "EU's Right to Be Forgotten: Guardian Articles Have Been Hidden by Google," *The Guardian*, July 2, 2014, sec. Comment is free, http://www.theguardian.com/commentisfree/2014/jul/02/eu-right-to-be-forgotten-guardian-google.

[160] Robert Peston, "Why Has Google Cast Me into Oblivion?," *BBC News*, July 2, 2014, www.bbc.com/news/business-28130581.

[161] These takedowns were seen by some as a deliberate media strategy by Google. Intentional or not, after receiving a lot of criticism for these takedowns, the company quickly reinstated the references. For more information, see: Chris Moran, "Things to Remember about Google and the Right to Be Forgotten," *The Guardian*, July 3, 2014, sec. Technology, http://www.theguardian.com/technology/2014/jul/03/google-remember-right-to-be-forgotten; Paul Bernal, "Facebook, Google and the Little People....," *Paul Bernal's Blog*, July 4, 2014, http://paulbernal.wordpress.com/2014/07/04/facebook-google-and-the-little-people/; David Meyer, "Why Is Google Really Removing Links to News Articles in Europe?," July 3, 2014, http://gigaom.com/2014/07/03/why-is-google-really-removing-links-to-news-articles-in-europe/; Andrew Orlowski, "Google de-Listing of BBC Article 'Broke UK and Euro Public Interest Laws' - So WHY Do It?," *The Register*, July 4, 2014, theregister.co.uk/2014/07/04/google_peston_bbc_delisting_not_compliant_w_public_interest_law_says_expert/.

EU. In other words, the form is not available outside the EU and search results are not filtered when queries are made on top-level domain names outside of the EU (e.g. .com; .sn).[162]

D. Looking ahead

It is still too early to draw conclusions about the eventual impact of the Google Spain ruling. Further observations and research should make a distinction between first and second order effects. First order effects relate to the implementation of the judgment in the EU. Second order effects relate to the broader consequences and implications (e.g. on innovation, freedom of expression, or the effect of this judgment outside of the EU).

Data protection regulators – both at the national and pan-European level – are arduously working on developing a 'dashboard' or 'platform' that should ensure a proper balancing between all interests at stake.[163] A critical element in this exercise is the development of *objective* criteria that could be applied the same across the EU (in order to harmonies the implementation of the ruling).[164] At this stage, it is worth noting that at least some official organizations (e.g. the French data protection authority, CNIL[165]; and the Council of the EU[166]) suggest a gradual/subsidiary approach where the data subject should first approach the source page before being able to go to the search engine.

Currently, there is still insufficient information to predict the second order effects. For example, there is not enough data on specific cases and corresponding compliance rates[167] to evaluate the impact on the right to freedom of expression, or innovation. As mentioned before, we should be prudent in predicting the possible impact of the judgment on the right to freedom of expression.

---

[162] This has also enabled some to compare search results (based on name-searches) in different jurisdictions and create a list of those results that have been the subject of an erasure request. See: Kevin Rawlinson, "'Hidden From Google' Lists Pages Blocked by Search Engine," *BBC News*, July 15, 2014, http://www.bbc.com/news/technology-28311217; Julia Powles and Luciano Floridi, "A Manifesto for the Future of the 'Right to Be Forgotten' Debate," *The Guardian*, July 22, 2014, sec. Technology, http://www.theguardian.com/technology/2014/jul/22/a-manifesto-for-the-future-of-the-right-to-be-forgotten-debate.

[163] Article 29 Working Party. "Press Release: Follow-up to the Ruling of the Court of Justice of the EU of 13 May 2014 on the 'Right to Be Forgotten,'" September 18, 2014. http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140918_wp29_press_release_97th_plenary_cjeu_google_judgment__17sept_adopted.pdf.

[164] A concrete example of such a criterion would be the admission of a removal request when the requestor's criminal record is expunged. Arguably, the societal goal of allowing people to start afresh after certain periods of time, would be rendered useless if reports on the underlying facts pop up among the first results when searching for a person's name.

[165] http://www.cnil.fr/linstitution/actualite/article/article/comment-effacer-des-informations-me-concernant-sur-un-moteur-de-recherche/

[166] Council of the European Union - Working Group on Information Exchange and Data Protection (DAPIX). "Note on the Proposal for a General Data Protection Regulation - the Right to Be Forgotten and the Google Judgment," July 3, 2014. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011289%202014%20INIT, 7.

[167] The only data available at the time of writing are the numbers communicated by Google to the Article 29 Working Party on July 31st, 2014. In this document, the search engine said to allow just over half of the removal requests it had received. See: Fleischer, Peter. "Questionnaire Addressed to Search Engines by the Article 29 Working Party Regarding the Implementation of the CJEU Judgment on the 'right to Be Forgotten,'" July 31, 2014. https://docs.google.com/file/d/0B8syaai6SSfiT0EwRUFyOENqR3M/preview.

First of all, a search engine's search results are very dynamic in nature and change constantly based on a plethora of factors (of legal,[168] economic,[169] or technical[170] nature) already. Secondly, the relevant webpage will still be findable through other – more specific – search terms (not including the name) and via other routes (e.g. different search engines, social networks, direct access, etc.). After all, we should not (over-)rely on one tool or service to constitute our (sole) window to all online information. At the same time, the judgment might encourage certain governments outside the EU to introduce more content control.

Finally, the CJEU's ruling in *Google Spain* will undoubtedly have an impact on the currently on-going legislative reform of the European data protection framework.[171] The Court seems to prompt legislators to be clearer in defining the distribution of responsibilities among different online actors, as well as providing better guidance on the potential conflict with freedom of expression (and other fundamental) rights and interests. This was also echoed in the Council of the EU's report on the *Google Spain* Ruling, specifically calling for the legislator's attention to "(1) the scope of the right [to be forgotten], (2) the grounds on which this right can be exercised, (3) the need to balance this right with the freedom of expression, and (4) whether there is still a need to impose an effort obligation on initial controllers to inform second controllers of the request for erasure of data."[172]

VI. Conclusion

The EU regime regarding liability of online intermediaries is in need of reform. The planned Notice and Action Directive failed to reach the EU Parliament before the 2014 elections. It is to be seen whether the review of the intermediary liability regime remains on the agenda of the new Commission.

This working paper made a deep dive into the situation of search engines in the European intermediary liability regime, with a particular focus on their position vis-à-vis data protection laws. From this analysis it became clear that the situation is far from resolved. First of all, the position, role, and scope of activities of search engines is very hard to categorize. Given their inherently editorial functions on the content they refer to, they cannot just be compared to more 'traditional' online intermediaries that remain more 'neutral' with regard to the content on their platforms/networks. The uncertainty about their position is also reflected in the widely diverging regulation of these online service providers throughout the EU. This complexity is only amplified by the fact that most (of the biggest) search engines are actually U.S. businesses. The *Google Spain* ruling in particular – although focusing specifically on data protection issues – highlights the need for a pan-European approach to the regulation of search engines.

---

[168] E.g. Child pornography, intellectual property protection.

[169] E.g. Public image of the company, advertisement, business model.

[170] E.g. Optimalisation, fraud/spam prevention.

[171] See: http://ec.europa.eu/justice/data-protection/review/index_en.htm.

[172] Council of the European Union - Working Group on Information Exchange and Data Protection (DAPIX). "Note on the Proposal for a General Data Protection Regulation - the Right to Be Forgotten and the Google Judgment," July 3, 2014. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011289%202014%20INIT.

Appendix B:
Online Intermediaries in India

NoC Online Intermediaries Case Studies Series: Online Intermediaries in India

Chinmayi Arun and Sarvjeet Singh
National Law University

Editorial Note: Context, Character, and Purpose of the Case Study

This case study is part of a globally coordinated, independent academic research project by the Global Network of Interdisciplinary Internet & Society Research Centers (NoC). Facilitated by the Berkman Center for Internet & Society at Harvard University, the project is the first output of a larger policy-oriented research initiative that examines the rapidly changing landscape of online intermediary governance at the intersection of law, technology, norms, and markets. In concert with other research projects, it seeks to develop criteria, comparative methods, and a shared data repository, and to compile insights and lessons learned across diverse communities of knowledge aimed at informing and improving Internet policy-making globally.

The initial research output consists of a case study series exploring online intermediary liability frameworks and issues in Brazil, the European Union, India, South Korea, the United States, Thailand, Turkey, and Vietnam, and a synthesis paper that seeks to distill key observations and provide a high-level analysis of some of the structural elements that characterize varying governance frameworks, with a focus on intermediary liability regimes and their evolution.

The authors of these case studies have participated in a multi-step process of in-person consultations and remote collaborations among a global team of researchers from the Network of Centers. Additionally, the case studies are based on a set of broader questions regarding the role of online intermediaries in the digital age.[1]

The research effort is grounded in a diversity of global perspectives and collaborative research techniques, committed to objective and independent academic standards, and aspires to be useful, actionable, and timely for policymakers and stakeholders. More broadly, the Network of Centers seeks to contribute to a more generalized vision and longer-term strategy regarding the role of academic research, facilitation and convening, and education and communication in the Internet age. For additional information on the initiative, please contact Urs Gasser, Berkman Center for Internet & Society, at ugasser@cyber.law.harvard.edu

[1] The process is documented at: "Online Intermediaries: Functions, Values, and Governance Options", The Global Network of Internet & Society Research Centers, 2014 https://drive.google.com/file/d/0B_ToTBKP5ITVWTl0UzV0U3B2RlU/view?usp=sharing.

Abstract: This case study maps and analyzes online intermediary liability in India. It begins with the landscape of online intermediaries in India, highlighting intermediaries of special interest. This includes, for instance, platforms used to arrange marriages, which are much more popular in India than dating platforms because of Indian social norms. The second section of the paper attempts to map in detail the governance mechanisms applicable to online intermediaries in India – this includes the licensing system used for internet service providers, the Information Technology Act, and the Copyright Act. The likelihood of generally applicable criminal law in India (such as the Indian Penal Code) as a potential source of intermediary liability is also discussed briefly. The final part of the paper assesses the impact of the governance framework, ties together its different themes of content blocking, interception of data, and notice and takedown of content. It analyzes the law under which these activities take place, from the perspective of good governance principles such as transparency and accountability. It also considers whether the governance framework for online intermediaries treats online speech in a manner that is consistent with the Indian constitution. The serious flaws in the systems followed in India are apparent through this assessment – the lack of transparency and accountability suggest that over-regulation of constitutionally protected speech is likely to result in very little protection of primary speakers' rights.

Table of Contents

I. Introduction

The intermediary eco-system in India is still evolving. At a glance, it is apparent that the major online intermediaries in India are familiar global names. This is not surprising given the demographic that is currently accessing the Internet in India: digital access is concentrated in urban areas, and among literate people who are familiar with the languages used by international online platforms.

This paper begins with an attempt to outline the significant online intermediaries operating in India and the market share held by each. It also highlights some interesting online intermediaries, like CGNet Swara, that are significant for reasons other than market share. CGNet Swara is a hybrid platform catering to parts of rural India, allowing tribal people to create news reports using a simple voice mobile phone connection. Indian social norms also generate their own versions of global online platforms. While dating websites are ubiquitous globally, their Indian counterparts focus on 'arranging' marriages using criteria like caste, religion and skin-color, which are significant factors in what is referred to popularly as the 'marriage market'.

The second part of the paper discusses the regulatory framework that governs intermediary liability in India. It outlines very briefly the constitutional framework within which intermediaries operate. It then proceeds to offer an indication of the criminal and civil liability that might apply to intermediaries without safe harbor protection. This safe harbor protection comes from the Information Technology Act, which offers conditional immunity to intermediaries. This immunity and the conditions attached to it – including intermediaries' obligations in the context of content blocking, interception of information, and notice and takedown – are discussed in some detail in this part. Also discussed is the Copyright Act's different safe harbor framework and the ex parte court copyright-infringement related orders that are increasingly prevalent in India.

The third part of this paper builds on the facts set out in the second part by offering an analysis, supported with data wherever possible, of the impact that the regulatory framework has on online intermediaries and the content that they are willing to host. This part of the paper considers the transparency and accessibility of the legal rules, in order to assess whether intermediaries are easily able to understand what they need to do to comply. It examines the framework's incentives to see whether a chilling effect is created. It also considers the transparency and accountability of government ordered blocking and interception to evaluate whether this liability regime offers any safeguards from censorship or surveillance by proxy.

The notice and takedown process set up under the Information Technology Act (IT Act) and the Copyright Act are controversial especially in terms of the chilling effect that they have on speech. Also of concern are several petitions currently before the Supreme Court of India. While some of these petitions seek to strike down the notice and takedown regime set up by the IT Act on grounds that it violates constitutional rights, others seek to reinstate a strict liability regime for obscene content online. The Supreme Court's ruling in these cases will shape the future of intermediary liability law in India. They are introduced at the end of this piece.

India currently has the world's third largest Internet consumer base after China and the United States,[2] with a total of 238.71 million subscribers as of December 2013[3] and 205 million users as of October 2013.[4] However, the number of active Internet users (i.e. users accessing the Internet at least once a month) was a much lower 149 million as of June 2013.[5] The users' engagement with the online space is also low, with Internet users in India spending only 20 to 25 hours on average online per month.[6]

A. Top Websites in India

The top websites in India, according to commercial web traffic data collected by Alexa, an analytical website, are as follows:[7]

S. No.	Top Websites in India
1.	google.co.in
2.	google.com
3.	facebook.com
4.	youtube.com
5.	yahoo.com
6.	wikipedia.org
7.	blogspot.in
8.	flipkart.com
9.	indiatimes.com
10.	linkedin.com
11.	twitter.com
12.	jabong.com

[2]Moulishree Srivastava, *Internet base in India crosses 200 million mark*, MINT (Nov. 13, 2013), http://www.livemint.com/Consumer/9pWsphmYL2YjdisfO7bGLM/Internet-base-in-India-crosses-200-million-mark.html.s

[3]Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators: April - June, 2013, xii, 27 (Dec. 2013), *available at* http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator%20Reports%20-%20Jun-02122013.pdf.

[4]*Internet Users in India Crosses 200 Million Mark*, IAMAI (Nov. 13, 2013), http://www.iamai.in/PRelease_detail.aspx?nid=3222&NMonth=11&NYear=2013.

[5]*IAMAI Internet in India 2013*, Internet and Mobile Association of India, 2 (2013).

[6] Chandra Gnanasambandam and Anu Madgavkar, *Online and upcoming: The Internet's impact on India*, MCKINSEY & COMPANY (Dec. 2012), *available at* http://www.mckinsey.com/insights/high_tech_telecoms_Internet/indias_Internet_opportunity.

[7]*Top sites in India*, ALEXA (July 24, 2014), *available at* http://www.alexa.com/topsites/countries/IN.

13.	amazon.com
14.	stackoverflow.com
15.	wordpress.com

Figure 1. *Top Websites in India*

This data indicates that thirteen of the top fifteen websites are based outside India. The two exceptions are flipkart.com (an online retailer that reaches markets similar to those targeted by Amazon) and indiatimes.com (a content portal owned by Indian media company Bennett, Coleman and Co. Ltd.).

1. Search Engines

S. No.	Name of Search Engine	Market Share (%)[8]
1.	Google	97.03
2.	Yahoo!	1.12
3.	Bing	0.77

Figure 2*. Search Engines (Data from StatCounter)*

2. Social Media Websites:

S. No.	Name of Social Media Site[9]	Market Share (%)[10]
1.	Facebook	81.16
2.	YouTube	5.68
3.	Twitter	4.77
4.	StumbleUpon	2.36
5.	Tumblr	1.84
6.	Pinterest	1.51
7.	NowPublic	0.78
8.	LinkedIn	0.71

[8] *Top 5 Search Engines in India from June 2013 to June* 2014, *available at* http://gs.statcounter.com/#all-search_engine-IN-monthly-201306-201406.

[9] The data combines Micro blogs, Social media; User generated content platforms types of intermediaries as provided in the guiding questions document.

[10] *Top 7 Social Media sites in India from June 2013 to June* 2014, *available at* http://gs.statcounter.com/#all-social_media-IN-monthly-201306-201406.

9.	Google+	0.63
10.	Reddit	0.46

Figure 3. *Social Media Websites (Data from StatCounter)*

Facebook has the largest user base in India with 93 million users, followed by Twitter with its estimated 33 million accounts,[11] and LinkedIn, which has 24 million users.[12] According to the Comscore India Digital Future in Focus Report 2013, Facebook is the most popular social media site in India, capturing the maximum screen time with access to 86% of the user base in India and 59,642,000 unique visitors in 2012-2013.[13] The report suggests that Facebook is followed by LinkedIn, which is the next most popular, with 11,127,000 visitors, followed by Twitter, which had 3,884,000 unique visitors.[14] An IAMAI report suggests that 96% of the total number of social media users use Facebook, while 57% use Google plus, and 49% use Orkut.[15] The video-sharing platform YouTube has over 55 million unique users a month in India,[16] and is used by 58% of 137 million Internet users in the country.[17]

B. Intermediaries of Interest in India

There are many intermediaries in India that were created in response to Indian social norms and markets. These include online matrimonial portals, which resemble online dating services in some ways, but have other design choices and actual functions that cater to Indian social norms. The first of these matrimonial portals began operation in 1996 and was called sagaai.com (subsequently shaadi.com),[18] owned by People Group. The online matrimony market is currently valued at around $83,000,000[19] and is expected to touch $250,000,000 by 2017.[20] In deference to widespread Indian practices about marrying within particular sub-groups, these portals enable

[11] Atish Patel, India's social media election battle, BBC NEWS INDIA (Mar. 31, 2014), http://www.bbc.com/news/world-asia-india-26762391.

[12] *LinkedIn India user base crosses 24 million; 277 million members worldwide*, NDTV (Feb. 12, 2014), http://gadgets.ndtv.com/social-networking/news/linkedin-india-user-base-crosses-24-million-277-million-members-worldwide-482512.

[13] *India Digital Future in 2013*, COMSCORE, 24 (Aug. 22 2013), *available at* http://www.comscore.com/Insights/Presentations_and_Whitepapers/2013/2013_India_Digital_Future_in_Focus.

[14] *India Digital Future in 2013*, COMSCORE, 24 (Aug. 22 2013), *available at* http://www.comscore.com/Insights/Presentations_and_Whitepapers/2013/2013_India_Digital_Future_in_Focus.

[15] *Social Media in India – 2013*, INTERNET AND MOBILE ASSOCIATION OF INDIA, 6 (Oct. 2013).

[16] N Madhavan and Vivek Sinha, *We have 10,000 full-length Indian movies on YouTube: Google India chief*, HINDUSTAN TIMES (Sept. 17, 2013), http://www.hindustantimes.com/business-news/we-have-10-000-full-length-indian-movies-on-youtube-google-india-chief/article1 1123030.aspx.

[17] Rohin Dharmakumar, *Is Google Gobbling Up the Indian Internet Space?*, FORBES INDIA (Jul. 22, 2013), http://forbesindia.com/article/real-issue/is-google-gobbling-up-the-indian-Internet-space/35641/0#ixzz38Kf8IuNP.

[18] Satrajit Sen, *Arranged marriages over the Internet were a laughable idea when Shaadi.com started*, INDIA DIGITAL REVIEW (Dec. 5, 2011), http://www.indiadigitalreview.com/interviews/arranged-marriages-over-Internet-were-laughable-idea-when-shaadicom-started-anupam-g-mitt.

[19] Harsimran Julka & Apurva Vishwanath, *Matrimony portals making serious efforts to counter rising tide of divorces, ensure lasting unions*, ECONOMIC TIMES (June 26, 2013), http://articles.economictimes.indiatimes.com/2013-06-26/news/40206906_1_portals-online-bharatmatrimony-com.

[20] *Online marriage business may touch Rs.1,500 crore by 2017: Assocham*, INDIA TODAY (Dec. 18, 2013), http://indiatoday.intoday.in/story/online-marriage-business-may-touch-rs-1500-crore-by-2017-assocham/1/331691.html.

users to search for matches based on religion, caste, mother tongue, horoscope, skin tone, vegetarianism, alcohol consumption, and smoking habits. They enable parents to set up profiles for their offspring, allowing for the fact that many families 'arrange' marriages for young people and see the choice of partner as a family decision rather than an individual one. The consequence of this can be a violation of privacy and professional embarrassment for people who find that a wedding profile has been created for them without their consent. However, it is difficult to find lawsuits or complaints about these incidents since they take place between close family members and are usually handled informally. A more serious and fairly common problem in the context of matrimonial websites is fraud. News reports suggest that there are multiple cases of women and their families being duped by men who use these platforms to extort money by misrepresentation or blackmail.[21] The Government has issued a press release reminding these intermediaries of their obligation to disable harmful and unlawful information when it is reported, and to appoint Grievance Officers to assist with this process.[22] The press release also mentions the Indian Computer Emergency Response team works with social networking websites to disable fake accounts, and that this is more easily achieved for social networking websites with offices in India.[23]

In non-urban India, new platforms are being set up to bridge the digital divide even though broadband connectivity is still not available in these regions.[24] These platforms include initiatives like CGNet Swara, Kanoon Swara, and Graam Vani. CGNet Swara allows people in rural areas of central India with majorities of tribal populations to submit and listen to audio news reports regarding the area. The initiative receives an average of 200 calls per day and is driving the emergence of online reports on local issues.[25] The Gram Vaani[26] operates a Mobile Vaani initiative that connects reports from mobile phone users to stakeholders including governments and NGOs using an interactive voice response system. In the state of Jharkhand, it has over 100,000 users that call 2000 times a day.[27]

---

[21] Sadaf Aman, Frauds and Cheats Rule Matrimonial Sites, New Indian Express, http://www.newindianexpress.com/cities/hyderabad/2014/11/24/Fraud-and-Cheats-Rule-Matrimonial-Sites/article2537595.ece, last visited on 8th January 2015.

[22] *Steps to Prevent Frauds by Social Networking Sites and Matrimonial Sites*, PRESS INFORMATION BUREAU (21 Feb., 2014) http://pib.nic.in/newsite/PrintRelease.aspx?relid=104142.

[23] *Steps to Prevent Frauds by Social Networking Sites and Matrimonial Sites*, PRESS INFORMATION BUREAU (21 Feb., 2014) http://pib.nic.in/newsite/PrintRelease.aspx?relid=104142.

[24] As of 2013 only 60 million of the 190 million total Internet users were from rural India: *IAMAI Internet in India 2013*, Internet and Mobile Association of India, 2 (2013); The teledensity in rural areas is approximately 43 percent as compared to 140 percent teledensity in urban areas: TRAI, *Highlights on Telecom Subscription Data as on 30th April, 2014*, Press Release No. 35/2014 (June 26, 2014), http://www.trai.gov.in/WriteReadData/PressRealease/Document/PR-TSD-Apr,14.pdf.

[25] *India: Use Mobile Technology to Bring News to Isolated Tribal Communities*, International Centre for Journalists, http://www.icfj.org/knight-international-journalism-fellowships/fellowships/india-using-mobile-technology-bring-news-is-0.

[26] *Graam Vaani: About Us*, http://www.gramvaani.org/?page_id=76.

[27] *How Mobile Vaani Works*", http://www.gramvaani.org/?page_id=15.

Online recruitment websites such as 'naukri.com' and 'monster.com' have also gained immense popularity in India.[28]

II. Governance Mechanisms and Legal Frameworks for Intermediary Liability in India

Online intermediaries are subject to a fairly complex regulatory framework in India, which leaves them open to civil and criminal liability. The most significant laws governing intermediaries may be found in the Information Technology Act, 2000, and the Copyright Act, 1957. However there are circumstances in which more generally applicable legislation, such as the Indian Penal Code (1860), the Scheduled Caste and Scheduled Tribe (Prevention of Atrocities) Act (1989), the Protection of Children from Sexual Offences Act (2012), as well as the law of torts, may apply. If an online intermediary is not eligible for immunity from liability offered by the IT Act,[29] it could incur civil or criminal penalties for offences such as defamation,[30] obscenity,[31] sedition,[32] and/or copyright claims.[33]

The regulatory approach thus far is largely command and control, as is typical of the Indian legal system. However, this seems to be changing gradually as the architectural constraints of the Internet become more apparent. Online intermediaries, unlike Internet service providers (ISPs), cannot be subject to the domestic licensing regime, given that several of them do not have offices in India and are therefore out of the physical jurisdiction within which the Indian Government is easily able to implement its laws. Therefore, although ISPs are subject to several obligations through their licenses (discussed below in 2.1), international online intermediaries remain free of these constraints.

A. Licensing System for Internet Service Providers

Internet service providers are required to get licenses in India, and are subject to several obligations through their license terms. Content intermediaries, however, do not have to get licenses for operation, and one of the reasons for this might be that it would be very difficult to enforce such a requirement on intermediaries located in other jurisdictions. Of the various types of Internet intermediaries, it is telecommunication service providers, network service providers, and Internet service providers that require a license to offer services in India.

The regulatory framework for intermediaries originates in the Indian Telegraph Act,[34] which empowers the Central Government to issue licenses to establish, maintain, or work a telegraph.[35] The Department of Telecommunication acts as a licensor on behalf of the Central Government,

---

[28] Rebirth of e-Commerce in India, Ernst and Young (2013), *available at* http://www.ey.com/Publication/vwLUAssets/Rebirth_of_e-Commerce_in_India/$FILE/EY_RE-BIRTH_OF_ECOMMERCE.pdf.

[29] The Information Technology Act, 2000, § 79 (prior to the Information Technology Amendment Act, 2008).

[30] The Indian Penal Code, 1860, § 499; *Khushwant Singh and Anr.* v. *Maneka Gandhi*, A.I.R. 2002 Delhi 58 (India); Ratanlal and Dhirajlal, The Law of Torts 279 (26th ed. 2013).

[31] The Indian Penal Code, 1860, § 292, The Information Technology Act, 2000, § 67.

[32] The Indian Penal Code, 1860, § 124A.

[33] The Copyright Act, 1957, § 51.

[34] The Indian Telegraph Act, 1885, § 4

[35] The Indian Telegraph Act, 1885, § 3 (1AA)

and enters into agreements with companies for the provision of telecommunications and Internet Services.

There are three types of licenses for communication providers in India:

- The License Agreement for Provision of Internet Services ('ISP License')[36]
- The License Agreement For Provision Of Unified Access Services after Migration from CMTS ('UAS License')[37]
- The License Agreement for Unified License ('Unified License')[38]

The Government has taken to issuing only Unified Licenses since 2012. This might be an effort to consolidate and simplify the licensing process, since the Unified License covers various telecom services such as access, Internet, and long distance within a single license.[39] It contains a separate chapter for Internet services.

The licenses obligate licensee-intermediaries to block Internet sites, Uniform Resource Locators (URLs), Uniform Resource Identifiers (URIs), and/or individual subscribers, as identified and directed by the government in the interest of national security or public interest from time to time.[40] The licenses also declare that carriage of objectionable, obscene, unauthorized, or any other content, messages, or communications infringing copyright and intellectual property rights etc., in any form, is not permitted, and obligates licensees to prevent such carriage when specific instances are reported.[41]

The license agreements contain a number of provisions concerning data retention, disclosure, and the provision of services to enable surveillance.[42] They require ISPs to put in place systems that enable lawful monitoring and interception of communications by the Indian Government.[43] ISPs are also required to trace or monitor content such as communications that are obnoxious, malicious, or a nuisance,[44] and 'objectionable' communications.[45]

---

[36] Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.
[37]Licence Agreement for Provision of Unified Access Services after Migration from CMTS , http://www.auspi.in/policies/UASL.pdf.
[38]License Agreement for Unified License , http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf.
[39] Department of Telecommunications, *Unified License*, http://www.dot.gov.in/licensing/unified-license
[40] Chapter IX clause 7.12, License Agreement for Unified License, http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf clause 7.12, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.
[41] Chapter V clause 38.1, License Agreement for Unified License, http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf clause 33.6, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.
[42] Chinmayi Arun and Ujwala Uppaluri, *Research Memorandum Concerning The Indian Surveillance Framework for iProbono* (2014).
[43] Chapter IX clause 8.1.1, License Agreement for Unified License, http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf.
[44]Clause 33.4, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.
[45] Clause 33.6, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.; Chinmayi Arun and Ujwala Uppaluri, *Research Memorandum Concerning The Indian Surveillance Framework for iProbono* (2014).

At every international gateway or node having an outbound capacity of more than 2 MB/s, ISPs are required to set up monitoring centers equipped with appropriate monitoring systems in accordance with government specifications,[46] office space,[47] telephone lines,[48] and be accessible to monitoring agencies at all times.[49] ISPs must also facilitate Government access to various equipment, leased lines, record files, and logbooks of the ISPs.[50] Additionally, periodic inspections of Internet leased line customers at their premise are to be performed by the ISP within 15 days of commissioning an Internet line to check for possible misuse.[51]

The UAS & Unified Licenses require licensee service providers to provide the 'necessary facilities' to the Government to "counteract espionage, subversive acts, sabotage, or any other unlawful activity."[52] All three licenses obligate licensees to 'facilitate' the application of Section 5 of the Indian Telegraph Act, which deals with interception of communication.[53]

B. The Information Technology Act, 2000

The Information Technology Act, 2000 (referred to as 'IT Act') came into force on October 17th, 2010 and was meant to provide legal recognition of *electronic commerce.*[54] It was also meant to give effect to a UN General Assembly resolution on Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law.[55] The IT Act was amended in 2008[56] in a manner that expanded the safe harbor protection significantly, thereby changing the intermediary liability regime substantially. The amendment emerged after the Report of the Expert Committee on the Proposed Amendments to the IT Act, 2000 suggested certain reforms, which would also ensure that the law relating to intermediary liability had more clarity and was closer to the framework in the EU E-Commerce Directive 2000/31/EC,[57] which was used to guide the revision of the IT Act.[58]

---

[46] Clause 34.27(a)(i), Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf. 34.27(a)(i)

[47] Clause 34.27(a)(ii), Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.

[48] Clause 34.27(a)(iii), Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.

[49] Clause 34.27, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf

[50] Clause 30.1, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.

[51] Clause 34.17, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.

[52] Clause 41.1, Licence Agreement for Provision of Unified Access Services after Migration from CMTS , http://www.auspi.in/policies/UASL.pdf

[53] Clause 40.1, License Agreement for Unified License, http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf; clause 35.1, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf; clause 42.1 Licence Agreement for Provision of Unified Access Services after Migration from CMTS , http://www.auspi.in/policies/UASL.pdf.

[54] The Information Technology Act, 2000, preamble (prior to the Information Technology Amendment Act, 2008).

[55] G.A. Res. 51/162, Model Law on Electronic Commerce, U.N. Doc. A/RES/51/162 (Jan. 30, 1997).

[56] The Information Technology (Amendment) Act, 2008.

[57] Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (June 8, 2000), *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:En:HTML.

[58] Department of Information Technology, Ministry of Communications & Information Technology, Government of India, Report of the Expert Committee on Proposed Amendments to Information Technology Act 2000, 46 (Aug. 2005), *available at* http://www.prsindia.org/uploads/media/Information%20Technology%20/bill93_2008122693_Report_of_Expert_Committee.pdf; Department of Information Technology, Ministry of Communications & Information TECHNOLOGY,

The IT Act, prior to amendment, protected intermediaries from liability[59] in a very limited manner. The immunity extended to a narrow set of intermediaries: it was provided only to a 'network service provider' which was defined as an intermediary, which in turn was defined as "any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.''[60] Additionally, protection was offered only with respect to offences committed under the IT Act, leaving intermediaries open to liability under other legislation for content that they hosted.

One of the concerns raised was that offering only 'network service providers' protection from liability might leave out a range of online intermediaries,[61] including the ones that provide online credit validation services.[62] It has also been argued that 'messages' were the only kind of content to which the safe harbor liability protection applied, and depending on how the term 'message' is interpreted, this may have narrowed the scope of the protection offered.[63] However, these concerns do not apply anymore, since the IT Act has been amended to expand both the immunity and the definition of the intermediaries that may claim this immunity.

Intermediaries with respect to electronic records are defined under the amended Section 2(w) of the Information Technology Act as "any person who on behalf of another person receives, stores, or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, Internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-marketplaces, and cyber cafes."[64]

This was hailed by some commentators for its wider and clearer definition of intermediaries, which unambiguously included online intermediaries within its purview.[65] Others have pointed out that that although this new definition expands the number of entities that can claim safe harbor protection under the IT Act, it fails to make allowances for the functional differences between the different kinds of intermediaries.[66]

Section 2(w) includes a variety of very different intermediaries, such as telecom service providers, network service providers, Internet service providers, web-hosting service providers,

---

Government of India, Summary of the Report of the Expert Committee on Proposed Amendments to Information Technology Act 2000, ¶ 17 (Aug. 2005), *available at* http://deity.gov.in/content/report-expert-committee-amendments-it-act-2000-3.

[59]The Information Technology Act, 2000, § 79 (prior to the Information Technology Amendment Act, 2008).

[60]The Information Technology Act, 2000, § 2, cl. w (prior to the Information Technology Amendment Act, 2008).

[61]Apar Gupta, Commentary on Information Technology Act 295 (2nd ed. 2011); Thilini Kahandawaarachchi, *Liability of Internet Service Providers for Third Party Online Copyright Infringement: A Study of US and Indian laws*, 12 J. I.P.R. 553, 559 (2007); Priyambada Mishra and Angsuman Dutta, *Striking a Balance between Liability of Internet Service Providers and Protection of Copyright over the Internet: A Need of the Hour*, 14 J. I.P.R. 321, 324 (2009); Pritika Rai Advani, *Intermediary Liability in India*, XLVIII (50) EPW 120 (Dec. 2013); *See generally* Aditya Gupta, *The Scope of Online Service Providers' Liability for Copyright Infringing Third Party Content under the Indian Laws- The Road Ahead*, 15 J. I.P.R. 35, 37 (2010).

[62]Apar Gupta, Commentary on Information Technology Act 295 (2nd ed. 2011).

[63]Apar Gupta, Commentary on Information Technology Act 295 (2nd ed. 2011).

[64] The Information Technology Act, 2000, § 2, cl. w.

[65]Aditya Gupta, *The Scope of Online Service Providers' Liability for Copyright Infringing Third Party Content under the Indian Laws- The Road Ahead*, 15 J. I.P.R. 35, 37 (2010).

[66]Pritika Rai Advani, *Intermediary Liability in India*, XLVIII (50) EPW 120, 122 (Dec. 2013).

search engines, online payment sites, online-auction sites, online-marketplaces or cyber cafes, in its scope. The obligations under the IT Act are such that all these intermediaries, online or offline, are subject to exactly the same legal regime.

Differential obligations may apply to different kinds of intermediaries owing to regulations that may be specific to their particular function, such as licenses for ISPs or banking regulations for financial intermediaries. However, the safe harbor protection for intermediaries includes immunity from liability under other legislations, and therefore intermediaries that meet the conditions for immunity in section 79 of the IT Act all get immunity and find themselves in a similar position regardless of their specific role or nature. It has been argued that by not taking into account the functional differences of the intermediaries, the efficacy of the immunity may be compromised.[67]

1. Safe Harbor, 'Due Diligence,' and Editorial Control

The amended safe harbor provision under Section 79 allows a wide spectrum of intermediaries to seek safe harbor protection from liability for any third party information, data, or communication link hosted by the third party. Section 79 ensures that the intermediaries' immunity from liability prevails over all other laws in force,[68] except for the Copyright Act and the Patents' Act.[69]

To be granted immunity under section 79, the intermediary must:

- Merely provide access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted;[70] or not initiate the transmission, select its receiver, or select or modify the information contained in the transmission;[71] and
- Observe due diligence[72] as provided by rules promulgated by the government in 2011.[73]

The use of the word "or" between the first two conditions stated above means that they are disjunctive in nature and only one needs to be satisfied in order for the intermediary to be granted immunity, along with fulfilling the third condition.[74]

Some commentators suggest that section 79 uses both the "mere conduit" and the "caching" principles, borrowed from the EU E-commerce Directive,[75] whereas others point out that the

[67]Pritika Rai Advani, *Intermediary Liability in India*, XLVIII (50) EPW 120, 122 (Dec. 2013).
[68]The Information Technology Act, 2000, § 79, cl. 1.
[69]The Information Technology Act, 2000, § 81.
[70]The Information Technology Act, 2000, § 79, cl. 2(a).
[71]The Information Technology Act, 2000, § 79, cl. 2(b).
[72]The Information Technology Act, 2000, § 79, cl. 2(c).
[73]The Information Technology (Intermediaries guidelines) Rules, 2011.
[74] *Super Cassettes Industries Ltd* v. *MyspaceInc,* M.I.P.R. 2011 (2) 303 (India).
[75] Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (June 8, 2000), *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:En:HTML; Pritika Rai Advani, *Intermediary Liability in India*, XLVIII (50) EPW 120, 121-22 (Dec. 2013).

language explicitly only discusses the mere conduit principle.[76] What is clear upon examination of section 79 is that to be eligible for immunity, the intermediary has to confine itself to transmission of information and not initiate transmission, select the receiver, or modify the information.[77] Services that would clearly be covered here because of their conduit function include telecommunications carriers, ISPs, and other backbone services.[78] However, caching services should also be included since they do fall within the definition of an intermediary under the amended IT Act (which includes those who store and host information),[79] and the immunity under section 79 seems to extend to all intermediaries with no specific exclusion of caching services. There is no reason why service providers who offer hosting services and do not fall afoul of the preconditions to the safe harbor protection should not qualify for immunity under section 79.

Wielding editorial control would almost certainly cause an intermediary to be excluded from the safe harbor protection. For one thing, it would amount to selection of information, such that the intermediary will fail one of the pre-requisites listed in Section 79(2).[80]

Controversially, the immunity from liability granted by section 79 is contingent upon intermediaries observing 'due diligence'.[81] This standard has been outlined in multiple cases, and the obligations that it entails are listed in detail in the Information Technology (Intermediaries

---

[76]Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, CENTRE FOR INTERNET & SOCIETY 20-23 (Apr. 10, 2012), *available at* http://cis-india.org/Internet-governance/intermediary-liability-in-india.

[77]*See also* Pritika Rai Advani, *Intermediary Liability in India*, XLVIII (50) EPW 120, 122 (Dec. 2013).

[78]Rajendra Kumar and Latha R. Nair, *Information Technology Act, 2000 and the Copyright Act, 1957: Searching for the Safest Harbor?*, 5 NUJS L. REV. 554, 562 (2012).

[79]S. 79. Exemption from liability of intermediary in certain cases.—(1)Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-section (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.
(2) The provisions of sub-section (1) shall apply if—
(*a*)the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
(*b*)the intermediary does not—
(*i*)initiate the transmission,
(*ii*)select the receiver of the transmission, and
(*iii*)select or modify the information contained in the transmission;
(*c*)the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.
(3) The provisions of sub-section (1) shall not apply if—
(*a*)the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;
(*b*)upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.
Explanation.—For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

[80]Aditya Gupta, *The Scope of Online Service Providers' Liability for Copyright Infringing Third Party Content under the Indian Laws- The Road Ahead*, 15 J. I.P.R. 35, 38 (2010).

[81]The Information Technology Act, 2000, § 79, cl. 2(c).

guidelines) Rules, 2011. The implications of this standard are discussed in more detail in the section on Intermediaries Guidelines below.

However, there are other ways in which even intermediaries that perform purely conduit or hosting services might find themselves liable, despite section 79. Section 79(3) limits the immunity offered by section 79, by outlining the circumstances under which an intermediary will be forbidden from claiming immunity:

- If the intermediary has conspired or abetted in the commission of the unlawful act.[82] This means that if the intermediary is involved in the commission of offence in any way then it cannot claim exemption from liability;
- Or upon receiving actual knowledge about any unlawful content the intermediary fails to remove the content alleged to be infringing.[83]

The precise meaning of 'actual knowledge' is unclear upon a bare reading of the statute – it is not defined in the IT Act,[84] and it remains unclear, for example, whether a notice from any private party would automatically imply that the intermediary under question now has 'actual knowledge' of the unlawful content. This is a standard discussed in more detail in the Intermediaries Guidelines, which also uses the 'actual knowledge' standard.

2. Information Technology (Intermediaries Guidelines) Rules, 2011

The Central Government notified the Intermediary Guidelines on April 11th, 2011, in exercise of the powers conferred by Section 87(2)(zg) read with Section 79(2) of the Information Technology Act, 2000. The most significant part of these rules is their definition of the term 'due diligence' as used within section 79(2) (c) of the IT Act.

The 'due diligence' obligations of intermediaries under the Intermediary Guidelines[85] include three broad categories of requirements that are relevant: (a) the publication of certain rules, policies and user agreements; (b) the obligation not to knowingly host, publish, or transmit infringing information; and (c) the obligation to take down infringing information upon receiving actual knowledge of it.

i. Publication of Rules, Policies, and Terms and Conditions

Intermediaries are required to publish rules and regulations, privacy policies, and user agreements,[86] which appears to be enforced through self-regulation.[87] The Intermediary Guidelines do, however, set out fairly detailed broad terms that need to be a part of the intermediaries' private agreement with users. The user agreements, rules, and policies must forbid the user from hosting, publishing, displaying, transmitting, or sharing any information:[88]

[82]The Information Technology Act, 2000, § 79, cl. 3(a).
[83]The Information Technology Act, 2000, § 79, cl. 3(a).
[84]Pritika Rai Advani, *Intermediary Liability in India*, XLVIII (50) EPW 120, 125 (Dec. 2013).
[85]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3.
[86]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3, cl. 1.
[87]John Braithwaite, *Enforced Self-Regulation: A New Strategy for Corporate Crime Control*,80(7) MICH. L. REV. 1466 (1982).
[88]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3, cl. 2.

- That is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, pedophilic, libelous, invasive of another's privacy, hateful or racially, ethnically objectionable, disparaging, or relating to or encouraging money laundering or gambling,
- Harms minors in any way;
- Impersonates another person;
- Belongs to another person and to which the user does not have any right;
- Infringes any patent, trademark, copyright, or other proprietary rights;
- Violates any law, among other things; or,
- Threatens the unity, integrity, defense, security, or sovereignty of India, friendly relations with foreign states, or a public order, or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting to any other nation.

ii. Hosting, Publishing, Transmitting, or Modifying Infringing Information

The intermediary is also required to refrain from *knowingly* hosting, publishing, transmitting, or modifying any information prohibited under Rule 3(2)[89] (as listed in 'a' above).

Concerns were raised about the ambiguity of these terms, since none of them are defined in the IT Act or in the Intermediary Guidelines. In response, the Parliamentary Standing Committee on Subordinate legislation has already asked the Ministry of Communications and Information Technology to incorporate definitions of all these terms within the Intermediary Guidelines, and to ensure that the Guidelines do not end up creating any new category of offence.[90]

iii. Disabling Prohibited Information Upon 'Actual Knowledge'

The intermediary, upon receiving actual knowledge, whether on its own or whether through a written communication from an affected person that infringing information is being stored, hosted, or published on its computer system, is obligated to 'disable' such information within 36 hours of obtaining such knowledge.[91]

This last requirement effectively creates a notice and takedown regime. Although the Ministry insists that this is a self-regulatory regime,[92] a study conducted by the Centre for Internet and Society, Bangalore has demonstrated that intermediaries over-comply and tend to take down even legitimate information when they are sent a notice.[93]

The Ministry of Communication and Information Technology argued before the Parliamentary Standing Committee that the requirement to 'act' within 36 hours means that intermediaries have

[89]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3, , cl. 3.
[90]Standing Committee on Subordinate Legislation, Thirty First Report on The Information Technology Rules (March 21, 2013), ¶ 25-26, *available at* http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf.
[91]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3, cl. 4.
[92]Standing Committee on Subordinate Legislation, Thirty First Report on The Information Technology Rules (March 21, 2013), ¶ 49, 55, *available at* http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf.
[93]Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, Centre for Internet & Society (Apr. 10, 2012), *available at* http://cis-india.org/Internet-governance/intermediary-liability-in-india.

to respond to and acknowledge the complaint within 36 hours of receiving it, and initiate appropriate action. Upon the Parliamentary committee's insistence that this position should be clarified in the rules, the ministry issued an official clarification that states this position.[94] It said that while the Grievance Officer acting on behalf of the intermediary must act on the complaint expeditiously, the maximum time for redress is one month from the date on which the complaint was received, in accordance with Rule 3(11).

Subsequently, on March 23rd, 2012, a motion to annul guidelines was moved in the Rajya Sabha (Upper House of the Parliament). The annulment was defeated.[95] However, the rules have been challenged before the Supreme Court of India.

3. Blocking Orders Under the IT Act

Section 69A of the IT Act empowers the Central Government to direct the blocking of access to online information, and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 contain the procedure to be followed[96] for blocking access to information. As will be apparent from reading the procedure below, there are few external checks and balances in this process: the different stages of review of blocking orders are all conducted by committees or individuals who are a part of the executive branch of the government, and since there is a prohibition on disseminating information about the blocking orders,[97] the entire process is very opaque.

These blocking orders may be directed at any government agency or intermediary. Although these orders can, in theory, be directed at any intermediary (including ISPs and online intermediaries), sources tell us that they are typically directed at telecommunication companies and ISPs. However, this is not exclusively so, since it appears that the government has issued section 69A blocking orders to online intermediaries.[98]

The language used in the IT Act does not permit blocking orders to be issued arbitrarily. Under section 69A, it is only when the Government is of the view that it is "necessary or expedient" so to do in the interest of "sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above",[99] that it can direct blocking access to information generated, transmitted, received, stored, or hosted in any computer resource.[100]

---

[94]Department of Electronics and Information Technology, Ministry of Communications & Information Technology, Government of India, Clarification on The Information Technology (Intermediary Guidelines) Rules, 2011 under section 79 of the Information Technology Act, 2000 (March 18, 2013), *available at* http://deity.gov.in/sites/upload_files/dit/files/Clarification%2079rules(1).pdf.

[95]Anupam Saxena, *Motion For Annulment of India's IT Rules Defeated In Rajya Sabha; IT Minister Promises Consultation*, Medianama (May 18, 2012), http://www.medianama.com/2012/05/223-motion-for-annulment-of-india%E2%80%99s-it-rules-defeated-in-rajya-sabha-it-minister-promises-consultation/.

[96]The Information Technology Act, 2000, § 69A, cl. 2.

[97]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 16; *Verizon Releases Transparency Report* (Jan, 22, 2014), http://newscenter.verizon.com/corporate/news-articles/2014/01-22-verizon-releases-transparency-report/.

[98] http://164.100.47.132/LssNew/psearch/QResult15.aspx?qref=151935.

[99]The Information Technology Act, 2000, § 69A, cl. 1.

[100]The Information Technology Act, 2000, § 69A, cl. 1.

The reasons for the blocking must be recorded in writing.[101] Intermediaries who do not comply with the requests can be punished with imprisonment of up to seven years and are also liable to pay a fine.[102]

Individuals cannot directly request the blocking of access to any content[103] and need to send their complaints to the "nodal officers" of the organizations in question.[104] The term "organizations" in India means ministries and departments of the Central Government, or any of the State, Union Territory, or other Central Government agency that may be notified.[105] After examining the complaint and being satisfied with the need to block access, the organization may forward the complaint through its nodal officer to the "Designated officer,"[106] who is appointed by the Central Government and is the only person under the act who can issue directions for blocking (apart from the courts).

All the requests received by the Designated Officer are to be examined by a committee[107] (referred to as 'Blocking Order Committee' in this paper) consisting of the designated officer and representatives from the ministries of Law and Justice, Home Affairs, Information and Broadcasting, and the Indian Computer Emergency Response Team (CERT-In)[108] within seven days.[109] The committee is required to examine the request and determine whether it is covered under the grounds mentioned in Section 69A and should give specific recommendations on the request received.[110] The designated officer is required to make an effort to identify the person to whom the information in the complaint belongs or the intermediary who has hosted the information, and give this individual or entity the opportunity to be heard.[111] The recommendations of the Blocking Order Committee are presented to the Secretary of the Department of Technology for approval.[112] This process may be bypassed in the event of an emergency, in which case the designated officer is authorized to examine the request and submit

[101]The Information Technology Act, 2000, § 69A, cl. 1.
[102]The Information Technology Act, 2000, § 69A, cl. 3.
[103]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 6.
[104]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 4.
[105] The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 2, cl. g. "Organisation" means – (i) Ministries/Departments of Government of India; (ii) State Governments and Union Territories; (iii) Any other entity as may be notified in Official Gazette by the Central Government.
[106]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 3.
[107]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 7.
[108]Constituted under the Information Technology Act, 2000, § 70B.
[109]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 11.
[110]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 8.
[111]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 8, cl. 1, cl. 2 and cl. 3.
[112]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 8, cl. 5 and cl. 6.

his recommendations to the Secretary,[113] who, if satisfied, can pass an interim decision to block access through a written and reasoned order.[114] However, this request has to be brought before the Blocking Order Committee within 48 hours of the blocking order by the Secretary[115] and on the basis of the recommendations of the committee, the Secretary may revoke his/her approval and ask for the blocked content to be unblocked.[116] It is important to note that by the time blocking orders come before the Review Committee, the content under question is already blocked in India. This raises questions about how the committee is able to view the actual content, which may include videos, blocked during its review.

The rules also provide separately for a Review Committee,[117] which is mandated to meet at least once in every two months to review whether the directions issued for blocking are in accordance with Section 69A(1).[118] If the Review Committee is of the opinion that the orders issued are not in conformity with Section 69A(1), it may set aside the blocking order and ask for the information to be unblocked.[119] It is important to note that by the time blocking orders come before the Review Committee, the content under question is already blocked in India. This raises questions about how the committee is able to view the actual content, which may include videos, blocked during its review.

The Review Committee for blocking orders does not have to review orders from Indian courts asking for the blocking of any information. In these situations, the designated officer is required to submit a certified copy of the court order to the Secretary and initiate action as directed by the court.[120]

4. Interception Under the IT Act

Section 69 of the Information Technology Act requires intermediaries to extend all facilities and technical assistance to intercept, monitor or decrypt information, provide information stored in a computer or provide access to a computer resource, when called upon to do so by the agency of the appropriate government as contemplated in Section 69. This clearly extends to online intermediaries. As stated above, intermediaries that fail to meet these obligations may be punished with imprisonment of up to seven years.[121]

---

[113]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 9, cl. 1.
[114]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 9, cl. 2.
[115]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 9, cl. 3.
[116]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 9, cl. 4.
[117] The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 2, cl. (i) read with the Indian Telegraph Rules, 1951, r. 419A.
[118]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 14.
[119]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 14.
[120]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 10.
[121]The Information Technology Act, 2000, § 69, cl. 4.

The power to order interception rests with both the Central Government and the State Governments. Officers specially authorized have the power to order interception, monitoring, or decryption of data under specified circumstances. An interception order can be passed if it is necessary or expedient to do so in the interest of sovereignty or integrity of India, the defense of India, the security of State, friendly relations with foreign states, a public order, for preventing incitement to the commission of a cognizable offence relating to the above, or for investigation of any offence.[122] Interception of online communication is subject to the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, and has to follow the process detailed in the legislation.

The order for interception must be issued by a competent authority[123] designated as the Secretary in charge of the Ministry of Home Affairs for Central Government,[124] or the Home department for States or Union Territories[125] as may be applicable. The competent authority is required to consider whether it is possible to acquire the necessary information by other means and to order interception only if this is not possible.[126] An interception order may only remain in force for up to a period of 60 days and cannot be extended beyond a total of 180 days.[127]

Interception orders are conveyed to intermediaries by a designated nodal officer who authenticates them and conveys them to the designated person within the intermediary[128] along with a written request to facilitate the interception.[129] The designated officer of the intermediary or person in charge[130] must acknowledge the interception order within two hours of receipt and has to facilitate interception.[131] Intermediaries need to send interception requests every 15 days for authentication to the nodal officer of government agency.[132]

[122]The Information Technology Act, 2000, § 69, cl. 1.
[123]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 3.
[124]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 2(d)(i).
[125]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 2(d)(ii)
[126]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 8.
[127]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 11.
[128]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 12.
[129]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 13.
[130]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 14.
[131]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 15.
[132]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 18.

Intermediaries are required to destroy all the records within a period of two months following the discontinuance of interception or monitoring, unless they are required for any ongoing investigation, criminal complaint, or legal proceedings.[133]

Section 69B of the IT Act empowers the Central Government to authorize a government agency to monitor and collect attributes of the content, such as the time and date of its sending, size, duration, route (including the location and identities of the points of origin and destination),[134] and the type of underlying service ("traffic data") in order to enhance cyber security or for identification analysis and the prevention of intrusion or spread of computer containment in India.[135] Intermediaries are obligated to provide technical assistance and extend all facilities to the authorized agency,[136] or risk imprisonment for up to seven years.[137] These detailed procedures and other safeguards for such orders are listed in the Information Technology (Procedures and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules 2009.

Like the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, these rules require an order from a competent authority. This order may however be issued for a range of cyber security purposes including, tracking cyber security breaches or incidents, identifying or tracking any person who has breached, or who is suspected of having breached or being likely to breach, cyber security,[138] and must contain the reasons issuing such direction.[139] A nodal officer has to receive the order and send it to the designated officer of the intermediary.[140] These safeguards are very similar to the safeguards outlined above for interception of information.

These rules also place obligations on the intermediary or the person in charge to put in place adequate checks to ensure that unauthorized monitoring does not take place[141] and make the intermediary liable for the actions of its employees in the case of unauthorized monitoring or the collection of data.[142]

C. The Copyright Act, 1957

The safe harbor protection provided to intermediaries under the IT Act is subject to section 81 of the IT Act which states that nothing contained in the IT Act shall restrict any person from

[133]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 23(2).
[134]The Information Technology Act, 2000, § 69B, explanation (ii) .
[135]The Information Technology Act, 2000, § 69B, cl. 1.
[136]The Information Technology Act, 2000, § 69B, cl. 2.
[137]The Information Technology Act, 2000, § 69B, cl. 4.
[138]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, r. 3(2).
[139]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, r. 3(3).
[140]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, r. 4(2).
[141]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, r. 5.
[142]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, r. 6.

exercising any right conferred under the Copyright Act.[143] If not for the safe harbor protection contained within the Copyright Act, intermediaries could be held liable under Section 51(a)(ii) for secondary copyright infringement: under this, any person who provides any place to be used for communication of work to the public for profit, where such communication constitutes a copyright infringement, may be held liable for the infringement.[144] This would ordinarily open intermediaries to liability in cases where they store information on their servers and/or transmit it onwards, particularly when the profit from advertising in relation to infringing content.[145]

However, a safe harbor has been included via section 52 of the Copyright Act, which states that "transient or incidental storage of a work or performance purely in the technical process of electronic transmission or communication to the public" shall not amount to copyright infringement; and that "transient or incidental storage of a work or performance for the purpose of providing electronic links, access or integration, where such links, access or integration has not been expressly prohibited by the right holder" is also not infringement, unless the intermediary has reasonable grounds for believing that such storage is of an infringing copy. It has been made clear that the immunity offered under section 52 is not meant to extend to deliberate storage of infringing information.[146] However the problem here is the interpretation of what amounts to reasonable grounds for belief that an intermediary is storing infringing content; the judiciary has, in the past, seen the insertion of algorithm-generated advertisements as an indication of knowledge of infringement.[147] Commentators point out that this standard will need to be discarded since it confuses physical space with the manner in which the Internet works.[148]

Like the IT Act, the Copyright Act makes its immunity for intermediaries conditional: the proviso to Section 52(1)(c) requires intermediaries to refrain from facilitating access to potentially infringing content for 21 days upon receiving a written complaint from the copyright owner about infringement that is taking place the transient or incidental storage that constitutes infringement. However, access to the content may be restored after 21 days unless a court order requiring the take down is received within a period of 21 days. This creates a notice and takedown regime where content needs to be removed at the behest of individual complaints. Unlike the IT Act, however, the Copyright Act explicitly authorizes the restoration of content in cases where a court has not endorsed the complaint.

This notice and takedown regime is mapped out more clearly in Rule 75 of the Copyright Rules of 2013. The rights holder has to give written notice[149] to the intermediary, including details about the description of work for identification,[150] proof of ownership of original work,[151] proof

[143]This position is affirmed by Super Cassettes Industries Ltd v. Myspace Inc, M.I.P.R. 2011 (2) 303 (India).
[144] The Copyright Act, 1957, § 51, cl. a(ii).
[145] Super Cassettes Industries Ltd v. Myspace Inc, M.I.P.R. 2011 (2) 303 (India); Aditya Gupta, *The Scope of Online Service Providers' Liability for Copyright Infringing Third Party Content under the Indian Laws- The Road Ahead*, 15 J. I.P.R. 35, 37 (2010).
[146]Ananth Padmanabhan, *Give Me My Space and Take Down His*, 9 I.J.L.T 2 (2013), *available at* http://www.ijlt.in/archive/volume9/Ananth%20Padmanabhan.pdf.
[147] Super Cassettes Industries Ltd v. Myspace Inc, M.I.P.R. 2011 (2) 303 (India).
[148]Ananth Padmanabhan, *Give Me My Space and Take Down His*, 9 I.J.L.T 15-16 (2013), *available at* http://www.ijlt.in/archive/volume9/Ananth%20Padmanabhan.pdf.
[149] The Copyright Rules, 2013, r. 75, cl. 2.
[150] The Copyright Rules, 2013, r. 75, cl. 2(a).

of infringement by work sought to be removed,[152], the location of the work[153] (which would be the specific URL), and details of the person who is responsible for uploading the potentially infringing work (if available).[154] Upon receiving such a notice, the intermediary has to disable access to such content within 36 hours.[155] In a departure from the Intermediaries Guidelines, and in a positive move for transparency, intermediaries that host content are required to display reasons for disabling access to anyone trying to access the content.[156] The intermediary is permitted, but not required, to restore the content after 21 days if no court order is received to endorse its removal.[157] It is then not required to respond to further notices from the same complainant about the same content at the same location.[158]

However, the regime under the Copyright Act is also not without its problems. Critics have objected to the narrowness of "transient or incidental storage," which is necessary to claim immunity from liability under the safe harbor provision. They have also objected to the process under Rule 75, pointing out that it should have required the intermediary to notify the person who uploaded or created the content, creating an opportunity for a response that will enable the intermediary to let the content remain as is.[159]

Also of concern are the vaguely worded court orders increasingly issued in the context of copyright issues. These "John Doe" orders – or "Ashok Kumar" orders as they are called in India – are used by copyright owners to get ex parte injunctions against unknown parties.[160] There was a point at which these orders were so broad that they could be interpreted as creating a positive obligation on all intermediaries to proactively remove the questionable content. An example of the language used is, "For the forgoing reasons, defendants, their partners, proprietors…servants, agents, representatives…other unnamed and undisclosed persons, are restrained from communicating without license or displaying, releasing, showing, uploading, downloading, exhibiting, playing, and/or defraying the movie "DEPARTMENT" in any manner without a proper license from the plaintiff."[161]

---

[151] The Copyright Rules, 2013, r. 75, cl. 2(b).
[152] The Copyright Rules, 2013, r. 75, cl. 2(c).
[153] The Copyright Rules, 2013, r. 75, cl. 2(d).
[154] The Copyright Rules, 2013, r. 75, cl. 2(e).
[155] The Copyright Rules, 2013, r. 75, cl. 3.
[156] The Copyright Rules, 2013, r. 75, cl. 4.
[157] The Copyright Act, 1957, § 52(1), proviso.
[158] The Copyright Rules, 2013, r. 75, cl. 6.
[159] Apar Gupta, *Copyright Rules, 2013 and Internet Intermediaries*, Indian Law and Technology Blog (March 22, 2013); http://www.iltb.net/2013/03/copyright-rules-2013-and-Internet-intermediaries/; Chaitanya Ramachandran, *A Look at the New Notice and Takedown Regime under the Copyright Rules 2013*, Spicy IP (Apr 29, 2013), http://spicyip.com/2013/04/guest-post-look-at-new-notice-and.html.
[160] Lawrence Liang, *Meet Ashok Kumar the John Doe of India; or The Pirate Autobiography of an Unknown Indian*, Kafila (May 18, 2012), http://kafila.org/2012/05/18/meet-ashok-kumar-the-john-doe-of-india-or-the-pirate-autobiography-of-an-unknown-indian/.
[161] Viacom 18 Motion Pictures v. Jyoti Cable Network and Ors, C.S.(OS) 1373/2012 (May 14, 2012), High Court of Delhi (India).

The Madras High Court in *M/s. R.K. Productions Pvt. Ltd. vs. Bharat Sanchar Nigam Limited & 19 others*,[162] clarified in June 2012 that an earlier interim injunction was granted only in relation to a particular URL where the infringing movie is hosted, and not to of the entire website (addressing the overbroad blocking that was taking place by ISPs in response to such injunctions). Further, the applicant is directed to inform the respondents/defendants about the particulars of URL where the infringing movie is kept. On such receipt of the particulars of the URL in question from the plaintiff/applicant, the defendants shall take necessary steps to block such URLs within 48 hours. The following year, in December 2013, the Delhi High Court passed an Ashok Kumar order, an ad interim ex parte injunction that applied to "unnamed and undisclosed persons" in relation to the display, duplication, and distribution of the film 'Dhoom 3.'[163] Recently, the Delhi High Court issued such an injunction prohibiting 472 websites[164] and other unknown ones from broadcasting 2014 FIFA World Cup matches, which it then reduced to a list of 219 upon an objection that several of the websites on the list did not belong there.[165]

III. Impact Assessment

The legal framework governing the liability of Internet intermediaries in India has to remain consistent with the Indian Constitution.[166] This means that the statutory framework under which intermediaries are liable to block, take down, intercept, and monitor content may be challenged if it violates the right to the freedom of speech and expression,[167] or the right to privacy (as read into the right to life and personal liberty,[168] the right to the freedom of speech, and expression by the judiciary[169]) granted by the Constitution. The regulatory framework is also subject to administrative law principles, derived largely from common law; meaning rules, notifications, and actions arising from legislations must remain within the scope of their parent statute and the constitution[170] and cannot usurp any function that rightfully belongs to the legislature.[171]

---

[162] *M/s. R.K. Productions Pvt. Ltd.* v. *Bharat Sanchar Nigam Limited & 19 Others*, C.S. (OS) 208/ 2012 (June 22, 2012), The High Court of Judicature at Madras (India).

[163] *Yash Raj Films Pvt Ltd* v. *Cable Operators Federation of India and Ors*, C.S.(OS) 2335/2013 (Dec. 2, 2013), High Court of Delhi (India).

[164] *Multi Screen Media Pvt Ltd* v. *Sunit Singh and Ors*, CS(OS) 1860/2014 (June 23, 2014), High Court of Delhi (India).

[165] Nikhil Pahwa, *World Cup 2014: 219 websites blocked in India, after Sony complaint*, Medianama (Jul 7, 2014), http://www.medianama.com/2014/07/223-world-cup-2014-472-websites-including-google-docs-blocked-in-india-following-sony-complaint/.

[166] India Const.

[167] India Const. art.19, cl. 1(a).

[168] India Const. art. 21.

[169] Kharak Singh v. State of UP, A.I.R. 1963 S.C. 1295 (India); Gobind v. State of Madhya Pradesh, (1975) 2 S.C.C. 148 (India); R Rajagopal v. State of Tamil Nadu, A.I.R. 1995 S.C. 264 (India),¶ 9; District Registrar &Collector v. Canara Bank, A.I.R. 2005 S.C. 186 (India), ¶ 39.

[170] Indian Express Newspapers (Bombay) Pvt. Ltd. v. Union of India A.I.R. 1986 S.C. 515 (India).

[171] Agricultural Market Committee v. Shalimar Chemical Works Ltd A.I.R. 1997 S.C. 2502 (India); Ujwala Uppaluri, *Constitutional Analysis of the Information Technology (Intermediaries' Guidelines) Rules, 2011*, CIS India Blog (Jul. 16, 2012, 09:45 AM), http://cis-india.org/Internet-governance/constitutional-analysis-of-intermediaries-guidelines-rules.

The technology actually used by intermediaries has had visible effects on speech,[172] and has resulted in over-blocking in the past. It does, however, appear that regulators take into account market concerns – these concerns are increasingly reflected in reports that discuss the formulation of the regulatory regime and in arguments made by the Government of India before the Supreme Court of India.[173]

The narrative in the earlier parts of this paper mapped out the different kinds of liability to which online intermediaries are subject in India. This includes criminal liability for several kinds of content, including content that is defamatory,[174] obscene,[175] or amounts to contempt of court.[176] The Indian Penal Code uses gatekeeper liability to regulate unlawful speech,[177] and this can make operations risky for intermediaries without immunity from liability under section 79 of the IT Act. Recent interpretations of the law by the Indian Supreme Court indicate that intermediaries may find themselves at risk despite the immunity offered by the IT Act. In January 2015, the Supreme Court passed an interim order in an ongoing case, requiring Google, Yahoo, and Microsoft to refrain from advertising or sponsoring any advertisement which would violate Section 22 of the Pre-Conception and Pre-Natal Diagnostic Techniques Act, 1994.[178] This interpretation seems to accept the argument made by the Ministry of Information and Communications that search engines, as intermediaries under the IT Act, owing to their 'due diligence' obligations, must block all content that breaches Indian laws. However since this is merely an interim order, there remains some chance that the Supreme Court will change its mind on the subject by the time the final judgment is delivered.

If the interim order represents the Supreme Court's stand on this subject, it may undo the beneficial effects of safe harbor protection for search engines. Intermediaries may have very little clarity about the kinds of content they need to weed out, given the different kinds of speech criminalized by multiple Indian statutes (indicative list in the table in Annexure 1). This makes intermediaries who exercise editorial control particularly vulnerable. The IT Act adds to the list

[172]Anupam Saxena, *Over 200 sites blocked in India after Sony's piracy complaint: Report*, Times of India (Jul. 7, 2014), http://timesofindia.indiatimes.com/tech/tech-news/Over-200-sites-blocked-in-India-after-Sonys-piracy-complaint-Report/articleshow/37961214.cms;OpenNet Initiative, Country Profile: India 304 (Aug. 9, 2012), *available at* http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-india.pdf.

[173]Standing Committee on Information Technology 2007-08, Parliamentary Report on the Information Technology (Amendment) Bill, 2006, 16 (Sept. 7, 2007), *available at* http://www.prsindia.org/uploads/media/Information%20Technology%20/scr1198750551_Information_Technology.pdf; Standing Committee on Subordinate Legislation, Thirty First Report on The Information Technology Rules (March 21, 2013), ¶ 77, *available at* http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf; Sarvjeet Singh, *A Blanket Ban on Porn will violate Articles 19 & 21 of the Constitution: Government informs the Supreme Court*, CCG at NLUD Blog (May 5, 2014), http://ccgnludelhi.wordpress.com/2014/05/05/a-blanket-ban-on-porn-will-violate-articles-19-21-of-the-constitution-government-to-the-supreme-court/.

[174]The Indian Penal Code, 1860, § 499.

[175]The Indian Penal Code, 1860, § 292, The Information Technology Act, 2000, § 67.

[176] The Contempt of Courts Act, 1971, §§ 2, cl. c and 12.

[177]Chinmayi Arun, N.U.J.S. L. Rev. (forthcoming 2014)

[178] Sabu Mathew George v. Union of India, W.P. (C) No. 341/2008, interim order (Jan. 28, 2015), Supreme Court of India (India)

of criminalized speech, creating new categories of offences punishable with imprisonment ('grossly offensive' information,[179] for example).

Online intermediaries with no editorial control are also in a precarious position, despite their greater access to immunity from liability. The safe harbor protection granted to them under the IT Act is conditional upon the intermediaries observing "due diligence,"[180] and on their removing unlawful content upon receiving "actual knowledge" of such content.[181] Interestingly, one outcome of section 79 has been that online intermediaries are immune from liability in contexts in which bookstores, traditional media, and publishing houses would have been found to be liable (such as hosting obscene content).[182] Even online intermediaries with immunity are required to refrain from *knowingly* hosting, publishing, transmitting, or modifying any information prohibited under Rule 3(2).[183] This list of prohibited information consists of a very wide range of content including content that is "grossly harmful," "harassing," "pornographic," "pedophilic," "libelous," "invasive of another's privacy," "hateful," "racially, ethnically objectionable," and "disparaging."[184] Many of these are categories of content that are not defined in Indian law at all.

Terms like 'defamatory' and 'obscene',[185] which are actually defined in other pieces of Indian legislation, are not defined in the Intermediary Guidelines. While this might not be a hardship for large online intermediaries like Google or Facebook that have the resources to hire a legal team, a start-up or small online intermediary may struggle to acquire the legal expertise to ascertain what is meant by all the terms listed in Rule 3. This makes Rule 3 an opaque and inaccessible rule from the intermediaries' perspective. Compliance with such an unclear standard is difficult. The Parliamentary Standing Committee on subordinate legislation has recommended that all these terms which are not defined in the IT Act be defined in the Intermediary Guidelines for the convenience of the intermediaries and the general public.[186] If this recommendation were executed, it would make for a more transparent rule.

Intermediaries that are subject to the licensing system in India have to contend with the added burden of onerous requirements that cover blocking, interception, and monitoring.

The architectural constraints of the Internet are becoming apparent to the government, which has moved from its command-control approach to the position that comprehensive and guaranteed blocking of information is impossible.[187] The current regulatory regime tries to leverage

[179]The Information Technology Act, 2000, § 66A.
[180]The Information Technology Act, 2000, § 79.
[181]The Information Technology Act, 2000, § 79.
[182]Chinmayi Arun, N.U.J.S. L. Rev. (forthcoming 2014).
[183]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3.
[184]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3.
[185]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3.
[186]Standing Committee on Subordinate Legislation, Thirty First Report on The Information Technology Rules (March 21, 2013), ¶ 25, *available at* http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf.
[187] Sarvjeet Singh, *A Blanket Ban on Porn will violate Articles 19 & 21 of the Constitution: Government informs the Supreme Court*, CCG at NLUD Blog (May 5, 2014), http://ccgnludelhi.wordpress.com/2014/05/05/a-blanket-ban-on-porn-will-violate-articles-19-21-of-the-constitution-government-to-the-supreme-court/; Sarvjeet Singh, *Cannot Block all Pornographic Material over the Internet: Centre informs the SC*, CCG at NLUD Blog (Aug 29, 2014),

intermediaries' existing capabilities by requiring them to make reasonable efforts to develop terms and conditions, as well as technological filters to regulate user-behavior. This looks like the beginnings of enforced self-regulation since it leaves the choice of technology and user agreements to the intermediaries after specifying the minimum terms or standards that need to be incorporated. However, it is not clear whether and how compliance is monitored in this context.

As it stands, under-resourced start-up companies may not be able to put in place a complex system to meet these standards, and making it risky to enter the market.[188] A Global Network Initiative study concluded that online intermediaries are burdened by costs and risks associated with the current legal regime in India, and that this regime has had a detrimental impact on established businesses and new ventures.[189]

There is very little transparency, and therefore limited accountability, in the process followed while blocking, intercepting, or monitoring content. This is detailed in the sections below.

A. Government-Ordered Blocking of Content

The Blocking Rules permit government agencies to ask for content to be blocked. Although these requests are most frequently directed at telecommunication companies and Internet service providers, they are also sent to online intermediaries from time to time. For example, social networking sites were asked to comply with court orders by blocking 8 URLS in 2010, 21 URLS in 2011, 352 URLs in 2012, and 1299 URLS from January 2013-2014.[190]

The government-ordered blocking process under the Blocking Rules is shrouded in secrecy – Rule 16 of the Blocking Rules requires that blocking requests and implementation be kept confidential. The effect is that the government is able to refuse to give out information about blocking,[191] and companies are restricted from making disclosures in this context. This is the reason that the January 2014 Verizon transparency report did not disclose the number of blocking requests from the Indian government, and explained that Indian law did not permit Verizon to make this disclosure.[192]

---

http://ccgnludelhi.wordpress.com/2014/08/29/cannot-block-all-pornographic-material-over-the-Internet-centre-informs-the-sc/.

[188] Martin Hvidt Thelleet. al., *Closing the Gap – Indian Online Intermediaries and a Liability System Not Yet Fit for Purpose*, Copenhagen Economics (2014), *available at* http://www.globalnetworkinitiative.org/sites/default/files/Closing%20the%20Gap%20-%20Copenhagen%20Economics_March%202014_0.pdf.

[189] Martin HvidtThelleet. al., *Closing the Gap – Indian Online Intermediaries and a Liability System Not Yet Fit for Purpose*, Copenhagen Economics (2014), *available at* http://www.globalnetworkinitiative.org/sites/default/files/Closing%20the%20Gap%20-%20Copenhagen%20Economics_March%202014_0.pdf.

[190] Reply by Mr. Kapil Sibbal, Minister of Communications & Information Technology, Government of India to Mr. Baijayant Panda, Member of Parliament, Starred question number 318 on Objectionable Content on Websites, LokSabha (Feb. 12, 2014), http://164.100.47.132/LssNew/psearch/QResult15.aspx?qref=151935.

[191] Reply to the RTI Application filed by Sarvjeet Singh at Centre for Communication Governance at National Law University, Delhi to the Department of Electronics and Information Technology, E-Security Division, (March 25, 2014).

[192] *Verizon Releases Transparency Report*, (Jan. 22, 2014), http://newscenter.verizon.com/corporate/news-articles/2014/01-22-verizon-releases-transparency-report/.

Since the system is opaque and does not require judicial or third party review or oversight at any point, it is reasonable to deduce that this may lead to reduced accountability. Government agencies ask for online content blocking through a process that is authorized, executed, and reviewed by the executive. Information about this blocking is not proactively disclosed by the government and cannot be disclosed by the intermediaries owing to Rule 16. The only mechanism to obtain the figures appears to be if a Member of Parliament asks for them in Question Hour.[193] Even the author or creator of the content, who might in theory have contested a blocking order on grounds of his/her constitutional free speech rights, has no way of contesting it since no reasons or notifications about the blocking of content need to be given to the creators or the audience of content.

In addition to the blocking requests that come from government agencies, court-ordered blocking of content also takes place under the IT Act. There is a Delhi High Court judgment confirming that 69A-blocking orders were sent to Google India Private Ltd. over the 'Innocence of Muslims' videos on YouTube.[194] 190 URLS were blocked over the videos as the Department of Electronics & Information Technology implemented orders from courts in Budagam, Ganderbal, Baramula, Srinagar, Anantnag in Jammu & Kashmir and courts at Akola, Bhiwadi, Mumbai, and Delhi.[195] 52 URLS of these videos were blocked under the Blocking Rules.[196]

Even the court orders, which are public documents in theory, are inaccessible in practice since many of them are obtained from remote regional courts. This also raises questions about how an intermediary might find the resources to travel to these locations and challenge any unreasonable blocking requests. Finally, since there is no mechanism to verify that each of the blocked URLS do in fact contain the content complained of, there is extensive potential for misuse of the blocking process.

At a meeting of the Cyber Regulation Advisory Committee, the Minister of Communications and Information Technology asked the Internet and Mobile Association of India, which is an industry association, to monitor and prepare a list of pornographic sites for blocking by the ISPs. The minister has suggested the need to understand United Kingdom system of installation of filtering software on home computers so that this may be replicated in India with modifications for the "Indian context."[197]

---

[193] Reply by Mr. Kapil Sibbal, Minister of Communications & Information Technology, Government of India to Mr. Baijayant Panda, Member of Parliament, Starred question number 318 on Objectionable Content on Websites, LokSabha (Feb. 12, 2014).

[194]Mohd. Amanullah & Ors. v. Union Of India &Ors., W.P. (C) No. 6325/2012 (Oct. 10, 2012), High Court of Delhi (India).

[195]Maulana Mahmood Asad Madani v. Union of India and Ors., W.P. (C) 7545/2012 (Jan. 24, 2013), High Court of Delhi (India).

[196]Maulana Mahmood Asad Madani v. Union of India and Ors., W.P. (C) 7545/2012 (Jan. 24, 2013), High Court of Delhi (India).

[197] Minutes of Meeting of the Cyber Regulation Advisory Committee, ¶ 14, (5 Sept. 2014), *available at* http://deity.gov.in/sites/upload_files/dit/files/Min-CRAC-5%20Sept.pdf; Jayadevan PK & Neha Alawadhi, *Government asks internet service companies to block pornography sites, upgrade systems,* THE ECONOMIC TIMES (Nov. 11, 2014), http://articles.economictimes.indiatimes.com/2014-11-11/news/55990473_1_internet-service-providers-internet-freedom-blocking-internet

This inclination towards blocking content is not, however, uniform within the Government. There are those who argue that filtering and blocking of content is a problematic solution. For example, a Secretary of the Ministry of Law and Justice stated in a Cyber Regulation Advisory Committee meeting[198] that, "it is not desirable to submit the plea to Supreme Court that it is difficult to filter or block pornography sites and we must try to evolve a solution."[199] Similarly, the Government has, in the past, told the Supreme Court that it is not technically feasible to block pornographic sites[200] and that doing so will be violation of Article 19 and 21 of the Indian Constitution.[201] It is, however, important to remember that this is not a consistent position and it is possible that the government will reverse its stance in the very same case once it comes up for hearing in February 2015.

B. Notice and Takedown

The safe harbor protection under section 79 of the IT Act is subject to the intermediary's removal of unlawful content immediately after receiving "actual knowledge" of it. The Intermediary Guidelines attempt to clarify what this phrase means, explaining that the intermediary could obtain such knowledge by itself or have such knowledge communicated to it by "an affected party in writing" or through an email signed by an electronic signature. After this, the intermediary is expected to "act within thirty six hours" to disable such information as it falls within the list of (undefined) prohibited content given in the Intermediary Guidelines. This has effectively created a notice and takedown regime for content.

The impact of these guidelines on intermediaries was demonstrated in a study conducted by the Centre for Internet & Society, Bangalore,[202] which tried sending frivolous notices to multiple intermediaries about perfectly legitimate content. The study found that intermediaries tend to remove even legitimate content in response to notices from private parties. A researcher sent take down notices to seven major intermediaries and found that six of these intermediaries over-complied. This offers some evidence to support the argument that the Intermediaries Guidelines might result in suppression of legitimate expression, since there is a visible chilling effect created by these guidelines. However the sample size for this study may be seen as problematic, and a larger investigation using the same method might be welcome.

The fact that intermediaries over-comply, disabling legitimate and legal content under the Intermediaries Guidelines is not surprising given the incentives created by the rules. Any failure to take down content places the intermediary at the risk of expensive litigation, but the rules do not require the intermediary to notify the author or user whose content has been taken down, or

---

[198] Established under the Information Technology Act, 2000, § 88.

[199] Minutes of Meeting of the Cyber Regulation Advisory Committee, ¶ 4, (5 Sept. 2014), *available at* http://deity.gov.in/sites/upload_files/dit/files/Min-CRAC-5%20Sept.pdf.

[200] Sarvjeet Singh, *Cannot Block all Pornographic Material over the Internet: Centre informs the SC*, CCG at NLUD Blog (Aug 29, 2014), http://ccgnludelhi.wordpress.com/2014/08/29/cannot-block-all-pornographic-material-over-the-Internet-centre-informs-the-sc/.

[201] Sarvjeet Singh, *A Blanket Ban on Porn will violate Articles 19 & 21 of the Constitution: Government informs the Supreme Court*, CCG at NLUD Blog (May 5, 2014), http://ccgnludelhi.wordpress.com/2014/05/05/a-blanket-ban-on-porn-will-violate-articles-19-21-of-the-constitution-government-to-the-supreme-court/.

[202] Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, Centre for Internet & Society (Apr. 10, 2012), *available at* http://cis-india.org/Internet-governance/intermediary-liability-in-india.

offer this speaker the right to defend his/her content or modify it such that it may legitimately stay online. The rules also do not contain any mechanism requiring intermediaries to make it clear to the audience that content has been taken down, making the entire system very opaque.

Bringing all these elements together, it is clear that the system for taking down content under the IT Act in India is very problematic because it (a) permits horizontal censorship by requiring intermediaries to respond quickly to any private citizen who may care to send them notice without any countervailing obligations towards authors or audiences; (b) obligates private intermediaries to make decisions about speech even when they are not performing an editorial function, and may lack the resources to make such determinations; and (c) ensures that there is no transparency at all about decisions to take down content, leading to a lack of accountability of private intermediaries for over-broad blocking and a lack of information based on which citizens may challenge particular instances of blocking.

The notice and takedown system under the Copyright Act might be marginally better in terms of transparency, since intermediaries are required to display a notice about why it was taken down.[203] The statute also permits (although it does not obligate) the intermediary to reinstate any content for which a court order is not received in 21 days.[204] This could, in theory, reduce the abuse of the notice and takedown system by private parties.

However this process is undermined to a great degree by the judiciary's practice of issuing ex parte 'John Doe' or 'Ashok Kumar' orders to disable allegedly infringing content. These orders would imply that the limitation on the period of the takedown would cease to apply. Critics point out that cases like *Multi Screen Media Pvt Ltd* v. *Sunit Singh*[205] indicate that the courts do not pay sufficient attention to the actual URLs that they are asked to block (the list of URLs had to be revised substantially; websites obviously wrongly named included Google Documents, which had to be removed from the original list).[206] Court-ordered blocks are only the tip of the iceberg. This is apparent when one considers for instance that *Multi Screen Media Pvt Ltd* v. *Sunit Singh*[207] is not Multi Screen Media's first sojourn into the realm content blocking. Google's transparency report for 2014 indicates that between February and July 2014, this company has made 77 removal requests to Google, covering a total of 27,624 URLs.[208] Out of these, 16,309 URLs were actually removed. In December 2014, 32 websites, including dailymotion.com, vimeo.com, and github.com were blocked as a result of a court order.[209] This led to controversy

[203] The Copyright Rules, 2013, r. 75, cl. 4.
[204]The Copyright Act, 1957, § 52(1), proviso; The Copyright Rules, 2013, r. 75, cl. 5.
[205]CS(OS) 1860/2014 (June 23, 2014), High Court of Delhi (India).
[206] Nikhil Pahwa, *World Cup 2014: 219 websites blocked in India, after Sony complaint*, Medianama (Jul 7, 2014), http://www.medianama.com/2014/07/223-world-cup-2014-472-websites-including-google-docs-blocked-in-india-following-sony-complaint/.
[207] CS(OS) 1860/2014 (June 23, 2014), High Court of Delhi (India).
[208]*Requests to remove content due to copyright violation by Multi Screen Media Private Limited*, Google Transparency Report (2014), http://www.google.com/transparencyreport/removals/copyright/owners/57964/Multi-Screen-Media-Private-Limited/.
[209] *Websites Blocked Following Court Order*, Press Information Bureau (Dec. 31, 2014) http://pib.nic.in/newsite/PrintRelease.aspx?relid=114259; http://cis-india.org/internet-governance/resources/2014-12-17_DoT-32-URL-Block-Order.pdf

owing to the apparent over-blocking of content.[210] After extensive negative publicity, the websites were unblocked.[211] The incident is a good illustration of the flaws of the court-ordered blocking system. The over broad blocking suggests that the judiciary may not have examined the contents of each URL and website on the list compiled for blocking.

Generally, in the period between July-December 2013, Google received 21 court orders for taking down content, affecting 118 items. It complied with 52% of these requests. It also received 133 requests affecting 422 items from other agencies (executive, police etc.) and complied with 23% of those requests.[212] These requests included one from an election candidate's representative for the removal of a YouTube video that allegedly connected the candidate with corrupt financial practices – Google denied this request since it not go through proper legal channels. Another such content removal request came from the local police and sought the removal of a blog post that contained content and pictures about a politician's sex scandal. This request was also denied, this time on grounds of the subjects of the blog post not being identifiable.[213]

During January-June 2014, Facebook restricted 4,960 pieces of content based on requests primarily by law enforcement officials and the Indian Computer Emergency Response Team.[214] During the same period, Twitter received no court orders and 5 requests from other agencies (executive, police etc.) to remove content. It complied with none of these requests, which involved 9 accounts.[215]

C. Interception of Information by Intermediaries

Section 69 of the Information Technology Act requires online intermediaries to extend all facilities and technical assistance to intercept, monitor or decrypt information, provide information stored in a computer, or provide access to a computer resource when called upon to do so by the government.

The interception of information under the IT Act follows a very detailed process in which attempts are made at various safeguards, such as designating senior officials for decision-

[210] Kim Arora, *Government blocks 32 websites to check ISIS propaganda,* The Times of India (Jan. 1, 2015), http://timesofindia.indiatimes.com/tech/tech-news/Government-blocks-32-websites-to-check-ISIS-propaganda/articleshow/45712815.cms; R. Jai Krishna, *India Orders Blocking of Websites for Alleged ISIS Content*, The Wall Street Journal (Jan. 2, 2015), http://www.wsj.com/articles/india-orders-blocking-of-websites-for-alleged-isis-content-1420032698; Jayadevan PK & Neha Alawadhi, *Government faces a firestorm of protests, decides to unblock some websites*, The Economic Times (Jan. 1, 2015), http://articles.economictimes.indiatimes.com/2015-01-01/news/57581476_1_websites-various-internet-service-providers-information-technology.

[211] Neha Alawadhi, *Government orders ISPs to unblock 32 websites, links*, The Economic Times (Jan. 10, 2015), http://economictimes.indiatimes.com/tech/internet/government-orders-isps-to-unblock-32-websites-links/articleshow/45829881.cms.

[212] *Requests to remove content from the Government of India,* http://www.google.com/transparencyreport/removals/government/IN/.

[213] *Requests to remove content from the Government of India- Explore Requests,* http://www.google.com/transparencyreport/removals/government/notes/?hl=en#authority=IN&period=Y2013H2.

[214] *Government Requests Report: India, https://govtrequests.facebook.com/country/India/2014-H1/*; *India tops Facebook's content restriction list*, The Economic Times (Nov. 5, 2014), http://articles.economictimes.indiatimes.com/2014-11-05/news/55798412_1_requests-facebook-january-june

[215] *Removal requests: India*, https://transparency.twitter.com/country/in.

making, creating review committees, and requiring intermediaries to check and only follow legitimately issued orders. However, at no point does it provide for third party oversight or transparency. The latter, in particular, may be far more effective in ensuring that no misuse of the system takes place than in relying on a busy senior official who may not have the time to properly judge the interception request, and are not accountable if they should end up authorizing an interception that they should not have.[216] Although the IT Act asks that interceptions not be authorized unless the information under question cannot be obtained by other means, it does not contain any procedural enforcement of this principle.

Online intermediaries are required to intercept information on the threat of imprisonment,[217] and they have to designate officers to meet the IT Act's detailed and cumbersome safeguards.[218] This process of designating a person and then ensuring that all the interception orders are received, are in the proper form, and are signed by the right parties may prove very difficult for new entrants.

Yahoo was actually fined 1.1 million Rupees (about US $22,000) when the company refused to hand over information related to about a dozen Yahoo IDs and IP addresses that the government wanted because it suspected these IDs were being used by Islamic terrorists or Maoists.[219] Yahoo refused the request, arguing that it was not made through the channels required by law, and that the fine was imposed by an entity (Controller of Certifying Authorities)[220] without any authority to impose it.[221] The fine was eventually retracted, but Yahoo was made to provide the information.[222]

Google received 2,513 user data requests regarding 4,401 accounts from the Indian Government between January and June 2013. Google handed over the information in 66% of the cases.[223] Facebook received a total of 3,598 requests regarding 4,711 accounts between July to December 2013 and it provided information in 53.56% of cases.[224] Twitter received 19 account information requests regarding 27 accounts and complied with 32% of these.[225]

In the absence of transparency, it is impossible for citizens to discover whether their information has been intercepted. As a result, they have no means at all of holding the state accountable for illegal interception of information.

---

[216]Chinmayi Arun, *Way to Watch*, Indian Express(June 26, 2013), http://archive.indianexpress.com/news/way-to-watch/1133737/.
[217]The Information Technology Act, 2000, § 69, cl. 4.
[218]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, r. 14.
[219]Controller of Certifying Authorities, available at http://cca.gov.in/rw/resource/CCA-ORDER-ISSUED-TO-YAHOO-DIGITALLTY-SIGNED.pdf?download=true.
[220] Appointed under The Information Technology Act, 2000, § 17(7).
[221]Yahoo India Pvt. Ltd. v. Union of India, W.P. (C) 6654/2011 (Sept. 14, 2011), High Court of Delhi.
[222]Yahoo India Pvt. Ltd. v. Union of India, W.P. (C) 6654/2011 (Sept. 14, 2011), High Court of Delhi; Chinmayi Arun and Ujwala Uppaluri, *Report on the Indian Surveillance Framework* (July 2014), prepared on behalf of iProbono for Privacy International.
[223]*Requests for user information from the Government of India* http://www.google.com/transparencyreport/userdatarequests/IN/.
[224]*Government requests report:* India, https://govtrequests.facebook.com/country/India/2013-H2/.
[225]*Information requests: India* , https://transparency.twitter.com/information-requests/2013/jul-dec.

IV. Cases currently before the Supreme Court[226]

A. Rajeev Chandrasekhar[227]

Rajeev Chandrasekhar, a member of the Rajya Sabha (the upper house of the Parliament of India) has filed a petition in the Indian Supreme Court challenging Section 66A of the Information Technology Act, 2000 and Rules 3(2), 3(3), 3(4) and 3(7) of the Information Technology (Intermediaries Guidelines) Rules, 2011 as violating Articles 14, 19, and 21 of the Indian Constitution.

1. Information Technology (Intermediaries Guidelines) Rules, 2011

The petition states that Rule 3(2) lists the various types of information that should not to be carried. This violates Article 14 of the Constitution, as these categories are arbitrary and overly broad. Moreover, the rules grant the private intermediary the right to subjectively assess objectionable content and create categories outside of the restrictions provided under Article 19.

Rule 3(4) of the guidelines provides the intermediary 36 hours to disable the information that is in contravention of Rule 3(2) when it receives such information on its own, or on the basis of information received. The petition argues that the period of 36 hours for removal of content is impractical and infeasible for intermediaries that process enormous quantities of data. The rules also require the intermediary to keep the offending information and associated records for at least 90 days, while Rule 3(7) calls upon the intermediary to provide any information or assistance to a Government agency seeking such information in writing. Both these rules violate the privacy under Article 21 of the constitution.

B. Common Cause[228]

Common Cause, an NGO along with senior Aam Aadmi Party leader and former Law Minister of Delhi Somnath Bharti has filed a writ petition in the Supreme Court of India arguing that Section 66A of the Information Technology Act, 2000, Section 69A of the IT Act and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 and Section 80 of the IT Act are in violation of Article 14, 19, and 21 of the Indian Constitution.

1. Section 69A and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

The petition puts forth various administrative law arguments that Section 69A of the IT Act and the 2009 rules framed under it violate the Constitution. It argues that the rules do not offer the creator or author of the content with a reasonable opportunity to be heard before blocking the

---

[226] Sarvjeet Singh, *Cases that will define the contours of Free Speech over the Internet in India*, CCG AT NLUD BLOG (Dec 10, 2014), https://ccgnludelhi.wordpress.com/2014/12/10/cases-that-will-define-the-contours-of-free-speech-over-the-internet-in-india/.

[227] Rajeev Chandrasekhar v. U.O.I. & Anr., W.P. (C) No. 23 (2013) (India), *available at* https://drive.google.com/a/nludelhi.ac.in/file/d/0B3Do3-9ZtwCrWnFKdTdLeXMwWlU/view.

[228] Common Cause (A Regd. Society) & Anr. v. U.O.I., W.P. (C) No. 21 (2013) (India), *available at* http://www.commoncause.in/whatsNew/8writpetition.pdf.

content. Additionally, there is no scope for a post-decision hearing, nor is there any provision to appeal the blocking order under the rules.

C. Moutshut.com[229]

Moutshut.com, a user review website, has filed a petition before the Supreme Court of India challenging the Information Technology (Intermediaries Guidelines) Rules, 2011, claiming that it violates Articles 14, 19, and 21 of the Indian Constitution.

The petition argues that sub-rule (2) of Rule 3 of the guidelines mandates intermediaries to place restrictions on the kinds of content that a user can post with a broad list of information that is highly subjective and can result in wide interpretation. Additionally, most of these terms are outside the reasonable restrictions provided under Article 19(2) of the constitution. The impugned rules result in the removal of any content that is disliked by any person or is not in his/her interest. The rules empower private parties to censor content over the Internet and places on them the burden to decide the lawfulness of the content, which should normally be a judicial function. The decision to take down content does not provide any opportunity to the owner of content to appeal, nor is the person informed.

D. Peoples' Union for Civil Liberties[230]

Peoples' Union for Civil Liberties, a human rights organization has filed a writ petition in the Supreme Court of India arguing that Section 66A of the Information Technology Act, 2000, the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 and the Information Technology (Intermediaries guidelines) Rules, 2011 are in violation of Articles 14, 19, and 21 of the Indian Constitution.

1. Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

The petition makes a number of arguments while arguing that the 2009 rules violate the Constitution. It argues that the rules do not offer the creator or author of the content a reasonable opportunity to be heard before blocking the content. The creator is not even informed about the content being blocked. There is no provision for a post decision hearing, or to appeal the blocking order under the rules. Additionally, there are no safeguards or guidelines provided, which need to be followed while making a decision.

2. Information Technology (Intermediaries guidelines) Rules, 2011

The petition argues that none of the terms under rule 3(2) of the intermediary rules are defined, and most of these terms are incompatible with Article 19(2). The rules are vague and ambiguous and do not provide the user reasonable opportunity to know what is permitted so that he/she may act according to law. The rules empower private entities to censor content over the Internet and place on them the burden to decide the lawfulness of the content without any legislative guidance, thereby forcing an adjudicatory role on an intermediary. The decision to take down

[229] Mouthshut.Com (India) Pvt. Ltd. & Anr. v. U.O.I. & Ors., W.P. (C) No. 217 (2013) (India), *available at* http://www.mouthshut.com/pdf/main_pitition.pdf.
[230] Peoples Union for Civil Liberties v. U.O.I. & Ors., W.P. (Crl.) No. 199 (2013) (India), *available* at https://drive.google.com/a/nludelhi.ac.in/file/d/0B_-V5K_jBhEXcmd1SmdVVFFGNDQ/edit.

content is made by the intermediary without hearing the party whose content is affected and without even notifying them of the removal.

Under these rules, similar content is treated differently across online and offline spaces. The rules also state that the intermediary has to take action upon a complaint by any affected person, however, who qualifies as an "affected person" has not be defined anywhere.

The petition also argues that the intermediary rules are ultra vires the parent statute as the guidelines formed under section 79 of the IT Act can only be related to 'due diligence' and the rules in their current form go a step further and legislate on various issues, including the information that can be posted online by a user, whereas the parent provision does not intend any prohibition.

E. Internet and Mobile Association of India231

Internet and Mobile Association of India, an industry body representing Internet platforms and businesses, has filed a writ petition in the Supreme Court of India arguing that Section 79(3)(b) of the Information Technology Act, 2000 is inconsistent with Articles 14 and 19 of the Constitution, and that the Information Technology (Intermediaries guidelines) Rules, 2011 are in violation of Articles 14, 19, and 21 of the Indian Constitution.

The petition states that the peremptory obligation on intermediaries under Section 79(3)(b) to disable or take down content is in violation of Articles 14 and 19 of the Constitution of India. According to the petition, Section 79(3)(b) deprives intermediaries of access to judicial recourse before removing material since intermediaries are required to take down unlawful material upon being notified by a private party or the Government. This violates the freedom of expression of the users and has a chilling effect on speech.

1. Information Technology (Intermediaries guidelines) Rules, 2011

The petition argues that the terms under rule 3(2) of the intermediary rules are vague and ambiguous and do not provide the user with reasonable opportunity to ascertain what is lawful content he/she may conform with the law. The petition also states that Rule 3(2)(b) is ultra vires Section 79(3)(b) of the IT Act since the rule goes beyond the legislative mandate of requiring intermediaries to disable content which is 'unlawful' and creates new categories of substantive ban. With respect to Rule 3(2)(f), the petition takes the view that it is ultra vires since it goes beyond the legislative mandate of requiring intermediaries to disable content that is 'unlawful'. It argues that this rule creates new categories of substantive proscriptions of speech that are not defined anywhere in Indian law.

The petition also argues that Rule 3(4) of the Intermediary Guidelines is in conflict with Section 79(3)(b), which requires an intermediary to act when allegedly unlawful information is brought to the "actual knowledge" of the intermediary. Rule 3(4) exceeds the limits of Section 79(3)(b) by making reference to the intermediary "obtaining knowledge by itself." The petition says that this language implies pro-active monitoring by an intermediary although Section 79(3)(b) of the IT Act does not obligate intermediaries to pro-actively monitor data/information unless it is

[231] Internet and Mobile Association of India & Anr. v. U.O.I. & Anr., W.P. (C) No. 758 (2014) (India), *available at* https://drive.google.com/a/nludelhi.ac.in/file/d/0B3Do3-9ZtwCrNnQzQTg5QmJFRjA/view.

brought to their attention by a third party or the Government. This rule is therefore seen as going beyond the scope of the parent provision and as an unreasonable requirement that is practically impossible to comply with given the volumes of data handled by intermediaries. Finally, the petition states that Rule 3(7) has the effect of circumventing the limitation placed on the State's power by Article 21 of the Constitution.

F. Kamlesh Vaswani[232]

Kamlesh Vaswani, an Indian advocate has filed a petition before the Indian Supreme Court, which seeks to declare sections 66, 67, 69, 71, 72, 75, 79, 80 and 85 of the Information Technology Act, 2000 as unconstitutional. It also asks the Government to frame a specific law and a national policy on pornography, to make viewing pornography an offence, and to direct intermediaries to proactively monitor and block all pornographic content on the Internet.

G. Sabu Mathew George

Sabu Mathew George,[233] a member of the National Inspection and Monitoring Committee constituted under the Pre-Conception and Pre-Natal Diagnostic Techniques (PCPNDT) Act, 1994, and his Non Governmental Organisation co-petitioner, Voluntary Health Association of Punjab, have filed a petition before the Supreme Court of India. The petition states that, the provisions of the PCPNDT Act, are being violated by various search engines as advertisements related to sex determination techniques and products are being displayed in India by these search engines.[234] It further asks that the Department of Electronics and Information Technology at the Ministry of Communications and Information Technology and the competent authority of Department of Health and Family Welfare work harmoniously to implement the provisions of the Act.[235] The petition is not publicly available and it is possible that it seeks other remedies that have not been reported in the media.

---

[232] Kamlesh Vaswani v. U.O.I & Ors., W.P. (C) 177 (2013), *available at* https://docs.google.com/a/nludelhi.ac.in/document/d/1ZyBevXbdC-FXzkSNA9itU5oFjhwO7CNSmZ7_H0Ji_B0/edit.

[233] Sabu Mathew George v. Union of India, W.P. (C) No. 341 (2008) (India)

[234] Shreeja Sen, *Nothing contrary to Indian laws should be advertised online: SC*, MINT (Dec. 5, 2014), http://www.livemint.com/Politics/5fGedpkVoAlvMQHd6nEopL/Nothing-contrary-to-Indian-laws-should-be-advertised-online.html.

[235] Sabu Mathew George v. Union of India, W.P. (C) No. 341/2008, interim order (Dec. 4, 2014), Supreme Court of India (India), *available at* http://supremecourtofindia.nic.in/outtoday/wc34108.pdf.

Appendix C:
Intermediary Liability – Not Just Backward but Going Back

NoC Online Intermediaries Case Studies Series: Intermediary Liability – Not Just Backward but Going Back[1]

Kyung-Sin (K.S.) Park
Korea University Law School

Editorial Note: Context, Character, and Purpose of the Case Study

This case study is part of a globally coordinated, independent academic research project by the Global Network of Interdisciplinary Internet & Society Research Centers (NoC). Facilitated by the Berkman Center for Internet & Society at Harvard University, the project is the first output of a larger policy-oriented research initiative that examines the rapidly changing landscape of online intermediary governance at the intersection of law, technology, norms, and markets. In concert with other research projects, it seeks to develop criteria, comparative methods, and a shared data repository, and to compile insights and lessons learned across diverse communities of knowledge aimed at informing and improving Internet policy-making globally.

The initial research output consists of a case study series exploring online intermediary liability frameworks and issues in Brazil, the European Union, India, South Korea, the United States, Thailand, Turkey, and Vietnam, and a synthesis paper that seeks to distill key observations and provide a high-level analysis of some of the structural elements that characterize varying governance frameworks, with a focus on intermediary liability regimes and their evolution.

The authors of these case studies have participated in a multi-step process of in-person consultations and remote collaborations among a global team of researchers from the Network of Centers. Additionally, the case studies are based on a set of broader questions regarding the role of online intermediaries in the digital age.[2]

The research effort is grounded in a diversity of global perspectives and collaborative research techniques, committed to objective and independent academic standards, and aspires to be useful, actionable, and timely for policymakers and stakeholders. More broadly, the Network of Centers seeks to contribute to a more generalized vision and longer-term strategy regarding the role of academic research, facilitation and convening, and education and communication in the Internet age. For additional information on the initiative, please contact Urs Gasser, Berkman Center for Internet & Society, at ugasser@cyber.law.harvard.edu

---

[1] The author has adapted significant portions of his argument from, "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], for the purposes of this case study. As a result, this study reflects both the essence of, and author's opinions from, the original piece.
http://m.riss.kr/search/detail/DetailView.do?p_mat_type=1a0202e37d52c72d&control_no=446c374bd83dd689ffe0bdc3ef48d419

[2] The process is documented at: "Online Intermediaries: Functions, Values, and Governance Options", The Global Network of Internet & Society Research Centers, 2014
https://drive.google.com/file/d/0B_ToTBKP5ITVWTl0UzV0U3B2RlU/view?usp=sharing.

Abstract: This paper provides an analysis of the Korean "Act Regarding Promotion of Use of Information Communication Networks and Protection of Information" that governs intermediary liability in Korea for defamatory or otherwise rights infringing content. This study makes the case that the Act's Article 44, 2, which should have created protection from liability like other intermediary liability regimes around the world, has become instead a way to impose intermediary liability in Korea. The paper also gives an overview of relevant court cases, the latest (2009) of which, in author's analysis, has had a "crushing" effect on protections from liability because it imposed liability for content that the intermediary was not aware of and was not given any notice of. This supports the argument that Article 44, 2 is unconstitutional because it imposes on intermediaries a *de jure* or *de facto* obligation to take down lawful content. Citing statistics on compliance with take down requests by the three major intermediaries in the country, the author observes that as a result of such liability-imposing regime the sheer volume of censorship has become problematic, and that politicians use requests to take down legal content that is critical of their policy decisions. This case also illustrates how intermediary liability rules that might seem benign are not necessarily so. To preserve the future of the Internet, rules that hold intermediaries responsible for removing unlawful content should be carefully considered before they are implemented. This case illustrates how Korea is a country where the special characteristics of the Internet are only considered for the sake of suffocating the power of the Internet.

Table of Contents

I. Introduction

This paper surveys South Korea's landscape for intermediaries, and analyzes the regulations thereon and their impact on society in general in response to the Network of Center's Guiding Questions on the Online Intermediaries research project. The author provides an overview of the country in section 2; discusses Korea's intermediary liability regime in section 3; presents their impact on the industry and society in section 4; follows how law and industry have dynamically interacted in section 5; and finally concludes with suggestions for the future.

II. Landscape for Korean Intermediaries

A. Market Survey

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%,[1] mobile Internet penetration rate of 75%, and Facebook penetration of 27%.[3] See below for comparison to Japan, U.S., and the world average.

	Korea	Japan	US	World average
Population	48 million	127 million	312 million	
Internet penetration	84%	79%	80%	52%
Mobile penetration	110%	109%	103%	93%
Internet mobile penetration	75%	48%	60%	21%
Facebook penetration	27%	17%	56%	

Figure 1. *Comparison of Internet use statistics.*

Korea's major intermediaries in each are as follows:

- **Search engines:** Naver, the local portal, has maintained 73% market share. Daum, the second largest local portal has roughly 21%, with Google covering the small remainder 3% (December 2012).[4]

- **Micro-blogging:** Twitter almost monopolizes the market, but if you include non-micro blogging, Naver still covers 80% of domestic bloggers.[5] In 2007, Naver already topped user visits per month[6] and its dominance grew over time ever since.

[3] 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).

[4] Ministry of Science, ICT and Future Planning and Korea Internet & Security Agency, 2013 Korea Internet White Paper, http://isis.kisa.or.kr/mobile/ebook2/2013/download/service.pdf, p. 180.

[5] There does not seem to be statistics tracking blogging or micro-blogging separately. "80%" is usually tossed around by Internet pundits who seem to derive that number from the search engine market share for the reason that bloggers are likely to expect search engines to promote the blogs on their own services and therefore likely to use the blog platform affiliated with the most popular search engine Naver.

[6] Nielson Korean Click Co., Ltd., "Domestic Blogging Services: Growth and Change", November 14, 2007 http://www.koreanclick.com/information/info_data_view.php?id=189.

- **Social Media:** 31.3% of all people use SNS (increase by 7.8% in 2013, fast-growing). Kakao Story[7] accounts for 55.4% of users, Facebook for 23.4%, Twitter for 13.1%, and Cyworld[8] (SK Communications) for 5.5% as of January 2014.[9] However, it is the author's opinion that Kakao Story numbers are exaggerated by the users who were given Story accounts by default due to their membership with Kakao Talk, the dominant private messaging service, which not really a social "networking" service. Weighing the time spent using the services, it seems to this author that Facebook is by far the most widely used social *networking* service in Korea. This is quite a change since 2010 when Cyworld accounted for 50% of social media users.[10] Leaving out the messaging services, the rankings are as follows:

    - **South Korea SNS 2014: Own an Account (Monthly Active User)**

        - Any SNS 84% (48%)
        - Facebook 75% (36%)
        - Twitter 56% (22%)
        - Google+ 38% (7%)
        - Me2Day 33% (7%)[11]

- **Private messaging:** Kakao Talk almost monopolizes the market.[12]

- **User Created Content:** YouTube has 75% but only in video content.[13]

- **Platform:** Google Play 75.2%, due to the dominance of Samsung (100% Android) in phone markets (Apple 17.9%, Blackberry and Windows each 4%).[14]

As part of the overall Internet economy, the mobile Internet is most often used for search (96.8%), then for SNS (50.4%), shopping (36.4%), banking (33.1%), etc. Time-weighted, it is used most for chatting (81.2%), phone calls (visual incl, 69.7%), texting (69.%), and searches (42.8%).[15]

---

[7] An *Instagram*-like SNS launched by *Kakao Talk*, the dominant private messaging service, opened

[8] A *My Space*-like service launched by the SK conglomerate. This remains the only non-telco intermediary founded by Korean *chaebol*s.

[9] Korea Information Society Development Institute, KISDI Stat Report "SNS Usage Analysis" (2013.12.26) http://www.kisdi.re.kr/kisdi/fp/kr/publication/selectResearch.do?cmd=fpSelectResearch&curPage=1&sMenuType=3&controlNoSer=43&controlNo=13270&langdiv=1&searchKey=TITLE&searchValue=sns&sSDate=&sEDate=

[10] Ministry of Culture, Sports and Tourism, http://m.korea.kr/newsWeb/ml/policyView.do?newsDataId=148703840&currPage=61.

[11] We Are Social Singapore, infra., p. 148

[12] Newsis, "Kakao Talk's Market Share at 92%. . Bandwagon Effects in Mobile Messenger Service, Twice That of Mobile Telecom", September 23, 2014, http://www.newsis.com/ar_detail/view.html?ar_id=NISX20140923_0013187317&cID=10402&pID=10400

[13] Newsis, "YouTube, Clearing the Video Market Thanks to Mandatory Identification Rule", October 9, 2013, http://www.newsis.com/ar_detail/view.html?ar_id=NISX20131009_0012419136&cID=10301&pID=10300.

[14] 2013 Korea Internet White Paper, infra, p. 29, http://isis.kisa.or.kr/ebook/WhitePaper2013.pdf.

[15] Korea Internet and Security Agency, "Year 2013 Mobile Internet Usage Survey", January 15, 2014. http://isis.kisa.or.kr/board/index.jsp?pageId=040000&bbsId=7&itemId=801&pageIndex=1.

As expected, the top uses of mobile Internet are not typical revenue-generators. Below are the revenues of top 10 Internet companies in Korea:

- **Top 10 Internet companies (by revenue)**
    - Naver (2.3 billion USD)
    - Nexon (1.6 B USD)
    - NCSoft (750 million USD)
    - NHN Entertainment (640 M USD)
    - eBay(640 M USD)
    - Daum (530 M USD)
    - Net Marle (497 M USD)
    - Neo Wiz (443 M USD)
    - Smilegate (360 M USD)
    - Wemade (227 M USD)[16]

Notice, out of 10 companies, the majority are game companies. Only Naver and Daum are portals. Facebook, Twitter (SNS), Kakao are not major revenue-generators. Google Play revenues are not significant, either.

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, 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 even prior to 2012, has become even more famous as it was 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 in 2012.[17]

In late 2014, the Korean intermediary Kakao Talk, the dominant messenger service provider, became the center of public attention when the Prosecutors' Office announced a new campaign to track down and indict the postings "causing division in national unity and skepticism of the government" for criminal defamation, and in doing so, mentioned Kakao Talk as a possible target for such search and seizure. This shocked the entire nation, 90% of who use Kakao Talk, because it has been a private messenger service connecting only those who knew each other. As a result, many 'migrated' to a foreign service, Telegram, whose server is located overseas, apparently safe from Korean authorities' search and seizure.[18]

---

[16] Blog 'Under the Radar', "2013 Internet Industry, Top 10 Revenue Generators", March 7, 2014, http://undertheradar.co.kr/2014/03/07/114-2013-%EC%9D%B8%ED%84%B0%EB%84%B7%EC%97%85%EA%B3%84-%EB%A7%A4%EC%B6%9C-top10/.

[17] New York Times, "Prosecutors Detail Attempt to Sway South Koran Election", November 21, 2013. http://www.nytimes.com/2013/11/22/world/asia/prosecutors-detail-bid-to-sway-south-korean-election.html?_r=0.

[18] BBC "Why South Koreans are Fleeing the Country's Biggest Social Network", October 10, 2014. http://www.bbc.com/news/blogs-trending-29555331.

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 if their operation "significantly hurts consumers' interests."[19] This environment creates a cloud under which the domestic companies feel the pressure to comply with even extra-legal guidance of the government. For instance, as you will read below, the "temporary take-down" regulation can be read as *optional* but effectively works as if it is mandatory, as do several other "optional" regulations, like the Korea Communication Standards Commission's "correction requests (to take down contents)"[20] and warrantless subscriber data requests. The compliance rates of these regulations were near 100% until a huge judgment came down on the latter in October 2012 in a consumer lawsuit filed by PSPD Law Center.[21]

D. Foreign Companies

The regulations, hard and soft, apply equally to Facebook, Twitter, Google, and Microsoft, which all have local offices but whose servers are located overseas, exempting the owners from local income tax liabilities. The extraterritoriality of the servers has also provided a rationalization for the fact that the government has not applied various intermediary regulations to these overseas providers, creating what domestic competitors decry as "reverse-discrimination."[22] The most infamous domestic-only regulation was a mandatory identity verification rule, which was snubbed only by overseas providers before it was struck down in 2012 in a constitutional challenge filed by PSPD Law Center.[23]

III. Korea's Intermediary Liability Regime

A. Intermediary Liability In General

What defines the Internet? The defining feature of the Internet is its structure 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

---

[19] Article 27 Paragraph 2 of the Telecommunications Business Act.

[20] See K.S. Park, "Administrative Censorship on Internet in Korea", http://opennetkorea.org/en/wp/administrative-censorship.

[21] See K.S. Park, "Internet Surveillance in Korea 2014", http://opennetkorea.org/en/wp/main-privacy/Internet-surveillance-korea-2014 I myself had the fortune of initiating and directing the legal campaign for the lawsuit, which is now pending in the Supreme Court.

[22] Business Korea, "Korean ICT Companies Suffering from Reverse Discrimination due to Governmental Regulations", http://www.businesskorea.co.kr/article/2274/%E2%80%9Creverse-discrimination%E2%80%9D-korean-ict-companies-suffering-reverse-discrimination-due.

[23] Constitutional Court's Decision 2010 Hunma 47, 252 (consolidated) announced August 28, 2012. K.S. Park, "Korean Internet Identity Verification Rule Struck Down" http://m.blog.naver.com/kyungsinpark/110145810944.

should be responsible for the content on their services. It is true that illegal activities such as defamation and copyright infringement that abuse the power of the Internet should be combated. However, unless society wants to paralyze the freedom of unapproved uploading and viewing – and therefore the power of the Internet – an intermediary should not be expected to know who posts what content and should not be held responsible for defamation or copyright infringements committed by content on its services. If intermediaries are held liable for this content, the intermediaries will have to protect themselves by constantly monitoring what gets posted on their services. If this happens, when a posting remains online it will appear to do so with the tacit consent of the intermediary in question. 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.[24] No common carrier would be in business if it were held liable for all the criminal conspiracies and deals taking place over its network. 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 is that the Internet companies carry the unlawful content on their servers, while the telecoms serve the contents *en route*. While some will surely abuse the free space created by these intermediaries, holding intermediaries liable merely for creating this space would be too threatening to the future of the Internet. Along this line of thought, on non-copyright-related matters the U.S. went further by claiming that no "interactive computer service" shall be considered a speaker or a publisher of such content.[25]

However, in other areas, many believe that there must be a limit on the exemption that intermediaries enjoy: 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 intermediaries always face a stronger incentive to take down content than to keep it up. The reason for this is that, first, intermediaries are massive content processors whose interest in individual pieces of content is small and, secondly, tort liability regimes around the world are usually such that the legal implications for keeping a posting up (a malfeasance) is always greater than the legal implications for removing it (a nonfeasance).

Therefore, many countries have decided to set up "safe-harbor" regimes where intermediaries are exempt from liability if they follow certain clearly defined procedures aimed at unlawful content. The most widely popular of such regimes is the notice-and-takedown regime,[26] whereby an intermediary is given an exemption from liability as long as it removes content when it is it is given notice of the content's infringing nature by the rights holder. Importantly, the notice-and-takedown safe harbor is not applicable to illegal content that the intermediaries have actual knowledge of before and/or without a notice provided by a rights holder or another person.

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

[24] Section 512 (a) of the Digital Millennium Copyright Act.
[25] 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**."
[26] DMCA section 512 (c) and (g).

safe harbors appears to have been misinterpreted: what Korea has is not an intermediary liability exemption regime but intermediary liability imposition regime. The relevant provisions of the 'Act Regarding Promotion of Use of Information Communication Networks and Protection of Information, Article 44-2 (Request to Delete Information)' are as follows:

- 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 a 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.
- 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
- Paragraph 6. The service provider may reduce or be exempted from 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, the exemption here is not mandatory, but is dependent on the Courts because the law states that the intermediary "may be reduced or exempted," rather than "shall be exempted." 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.

Indeed, historically, the predecessors of Article 44-2 (Article 44 Paragraphs 1 and 2 of the Network Act enacted 2001.7.16, Law No. 6360)[27] simply required the service provider to take down content upon the request of a party injured by that content and did not provide any exemption. Article 44 began as a simple idea that the service provider shall at least be responsible for content that is infringing if someone had complained about that content previously. Then, many service providers complained that they were not capable of determining

[27]"National Legal Information Center," n.d. http://www.law.go.kr/lsSc.do?menuId=0&subMenu=2&query=%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D#liBgcolor31.

whether certain content was infringing or not. In response, the law was amended in 2007 (Enacted 2007.7.27 Law No. 8289) into Article 44-2 to create a "temporary (blind) measure" for "border-line" content, so the service provider can now fulfill their responsibility under the previous law.[28] Together with that amendment, the noncommittal reference to possible "reduction or exemption" found its way into the law. The central idea that remained in each version was that the intermediary must remove infringing content upon demand.

The general idea of holding the intermediaries liable for *identified* infringing content seems innocuous, but the Korean case compellingly illustrates below why this should be abandoned.

C. On-Demand Takedown Obligations

As explained below, 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") states that service providers are required to take at least a "temporary measure" on *all* content upon which a takedown request has been made, regardless of the legality of the content.

The first possible interpretation is that the statute sets up such on-demand takedown obligations 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 a rights infringement has taken place. So the only feasible interpretation is that such obligation arises whenever someone *thinks and proposes* that his/her rights have been violated. Going further on this line of interpretation, this obligation can be filled by "temporary measure," but this is the minimum: the intermediary must take *some* abatement action. Now, the statute thus interpreted is in conflict with all known constitutions and international human rights treaties which allow freedom of speech to be violated only in favor of other protected rights or values.

Another more generous interpretation is possible: As you can immediately see from Paragraph 1 and 2, if someone complains of their infringed rights, the provider *must* take down the content if it is infringing. Now, there will be no problem if the takedown obligation applies only to that content that actually injures others. Indeed, Paragraph 1 limits its application only to "anyone whose rights have been violated." However, even if this is the case, the service providers will have a strong incentive to remove the content regardless, because otherwise the provider must risk being found in the wrong by courts and therefore being liable as a contributor to the dissemination of the infringing content. Usually, the service providers retain editorial control over the content through their Terms of Service so that they will not be held liable by the authors of the content for removing the content. Article 44-3 of the Network Act even codifies this rule.[29] On balance, the service provider always has a stronger incentive to take down content than to keep it up.

Now, Paragraph 4 states, in paraphrase, "the service provider may take a temporary measure (instead of permanent removal) if it is difficult to know whether the contents are infringing or when a dispute is expected between the parties." This should mean that, even if the content is

[28] "National Legal Information Center," n.d. http://www.law.go.kr/lsSc.do?menuId=0&subMenu=2&query=%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D#liBgcolor31.

[29] Article 44-3 The service provider may take a temporary measure voluntarily if it is recognized that the information circulated through the network operated and managed by the provider is infringing another's rights.

later found to be infringing, the service provider will not be held liable for the content if it has taken a temporary measure. While this seems to soften the de facto censorship effects of Paragraphs 1 and 2 by providing a less drastic alternative to a permanent removal, it does exactly the opposite. What is diabolical is that the permissive "may" in Paragraph 4 will encourage the intermediaries further to remove perfectly lawful content. This further aggravates the imbalance of incentives in favor of restricting content rather than keeping it up.

Make no mistake about it: under this second interpretation, the failure to take abatement action will result in liability only if the content is later found to be actually infringing. However, the intermediaries, not knowing for sure what content is infringing, will have strong incentives to take down even lawful content instead of risking being found liable later. Maybe a better expression of the dilemma is that the providers will be "chilled" into doing so, not because the concept "rights-infringing" is vague all the time, but because it is *vague ex ante.* On top of that, Paragraph 4 provides yet another incentive in favor of removing content by providing exemption from any liability for doing so.

Initially, the service providers were expected to gravitate away from permanent removals, for which there is no *ex ante* exemption, and toward temporary measures, for which there is *ex ante* exemption. This prediction turned out to be true. Naver, the number one content host, has often responded to all takedown requests with only temporary measures; Daum, the number two content host, eventually caught up in 2010.

In sum, contrary to the spirit of intermediary liability regimes around the world aimed at shielding the creators of online spaces from liability for what goes on in that space, Korean law ends up imposing de facto obligations on the intermediaries to censor lawful material, an obligation that did not exist before Article 44 or 44-2. The next section examines how courts dealt with intermediary liability before the current Article 44/44-2 regime.

D. Intermediary Liability in Court[30]

The Korean Supreme Court has ruled three times significantly on intermediary liability. In 2001, the Court held an electronic bulletin board provider liable for refusing, even upon demands both by the injury claimant and a government censorship body, to take down for a period of 5-6 months postings deprecating a pop singer's fan. The Court ruled that the intermediary had "a duty to take adequate measures when it knew or had reason to know of a defamatory posting."[31] This was a fairly typical case.

In 2003, when the Court was asked to find an intermediary liable for postings defaming a local politician, the Court took that as an opportunity to further limit when the duty to take adequate measures arises. [32] The Court held that an intermediary, even if it knew or had reason to know of the defamatory material for 52 days, should not be held responsible unless a comprehensive analysis of the following factors point to such responsibility: the posting's purpose, content, duration and method, the damages it has caused, the relationship between the speaker and the

[30] Woo Ji-Suk, "A Critical Analysis of the Practical Applicability and Implication of the Korean Supreme Court Case on the ISP Liability of Defamation" LAW & TECHNOLOGY, Vol.5, No.4: pp78-98. July 2009 http://plan2work.files.wordpress.com/2011/01/ebaa85ec9888ed9bbcec8690ec9790-eb8c80ed959c-ec9db8ed84b0eb84b7ec849cebb984ec8aa4eca09ceab3b5ec9e90isp-ecb185ec9e84-ec9ab0eca780ec8899.pdf.

[31] Supreme Court, 2001.9.7 Judgment, 2001Da36801

[32] Supreme Court 2003.6.27 Judgment, 2002Da72194

injury-claimant, the claimant's attitude, including whether rebuttal or takedown was requested, the size and nature of the site posted, the degree of for-profit nature of the site, when the operator knew or could have known the posting's content, and the technological and pecuniary difficulty in taking down, etc.[33] Having said so, the Supreme Court reversed the lower court decision that imposed liability for pre-takedown exposure. The Supreme Court's rather terse ruling sounds very generous, refusing to impose liability even upon knowledge of some indiscretion, especially given that this was before the exemption provision was added to Article 44-2. However, the ruling stands on the narrow fact that the intermediary here did comply immediately with the takedown request. Some said it made sense to require knowledge of the illegal character of the content.[34]

Then in 2009, a crushing judgment[35] came out where the Korean Supreme Court issued a decision holding web portal sites Naver, Daum, SK Communications, and Yahoo Korea liable for the defamation of the plaintiff when user postings on those sites accused him of deserting a girlfriend upon her second pregnancy after he had he talked her into aborting the first, after which the girlfriend committed suicide. The court upheld judgments of 10 million won, 7 million won, 8 million won, and 5 million won, respectively, against these services.

Specifically, the court held that (in paraphrase):

> Barring special circumstances, the intermediary shall be liable for illegal content to the same extent *as a news agency* and therefore shall be liable when (1) the illegality of the content is clear; (2) the provider was aware of the content; and (3) it is technically and financially possible to control the contents. On top of the duty to take down such content immediately, the intermediary has a duty to block similar postings later on. The Court will find the provider's requisite awareness under (2) above:
>
> a) When the victim has requested specifically and individually for the takedown of the content;
>
> b) When, even without such request, the provider was concretely aware of how and why the content was posted OR
>
> c) When, even without request, it was apparently clear that the provider could have been aware of that content.

The end result is that the intermediary will be absolutely liable for a posting later found to be "clearly" defamatory if "it was apparently clear that the provider could have been aware of that content" even if the victim did not notify the intermediary of the existence of the content.

This sets up what is probably one of the most strict intermediary liability regimes because it imposes liability for situations where content is "unknown but could-have-[been]-known."

---

[33] Supreme Court, 2003.6.27 Judgment, 2002Da72194.

[34] Hwang Sung-Gi, http://m.riss.kr/search/detail/DetailView.do?p_mat_type=1a0202e37d52c72d&control_no=12cb6a3625533040ffe0bdc3ef48d419.

[35] Please review a foreign scholar's response to this ruling. Anupam Chander, "How Law Made Silicon Valley" EMORY LAW JOURNAL [Vol. 63:639 (2014), http://www.law.emory.edu/fileadmin/journals/elj/63/63.3/Chander.pdf .

Anupam Chander plainly describes this ruling as stating that a web service "must delete slanderous posts or block searches of offending posts, even if not requested to do so by the victim."[36] It is true that the intermediary may be held liable for the content that looks clearly illegal *ex ante,* but should this liability exist even when the intermediary did not know?

True, DMCA notice-and-takedown immunity[37] does not apply to content that OSP had "actual knowledge" of the infringing nature of, or "awareness of facts or circumstances from which infringing activity is apparent." However, the DMCA is a safe harbor provision. It merely says that the safe harbor will not apply in case of "actual knowledge" or "awareness." It does not say that the OSP will be held liable in cases of such knowledge or awareness.

Furthermore, there is a world of difference between possible awareness – encompassed by the phrase "could have been aware" in the Korean ruling – on one hand, and "actual knowledge" or "awareness" on the other. The intermediaries, when facing such a liability regime, will have strong incentives to monitor *all* the content in order to make sure that there are no unknown clearly defamatory postings that it "could have been aware" of, but that they did not remove. This sets up a general monitoring obligation that kills the power of the Internet. Indeed, the Court does state that "[if the three conditions are met], the intermediary has a duty to take down such contents immediately AND block *similar* postings later."

What is more, this was not even a case interpreting the Article 44/44-2 regime because the cases here are concerned the intermediary's role when the victim did not make a takedown request, or before such a request was made. The Court was already ready to impose a *publisher*-like liability on the intermediary and a monitoring obligation.

IV. Result: Private Censorship

In summary, Article 44-2 states that all content should be taken down upon demand even if lawful. The Supreme Court decisions state that all unlawful content should be taken down even if unknown to the intermediaries. Together, the Court decisions encourage private censorship by intermediaries. On top of the censorship system triggered by private notices, Korean law provides for the Korean Communication Standards Commission which issues "correction requests" to all intermediaries, including telecoms, to take down or block domestically the content the Commission finds to be illegal. What is significant for now is that these injunctive functions, together with monetary damages, anticipated by the above-described liability regime, will provide stronger incentives to the intermediaries to take a heavy-handed approach toward censorship.[38] We will now look at some numbers and cases for illustration.

We will not look at copyright-related takedown notices, which may make up more than 90% of takedown requests in other countries, because the Korean Copyright Act sets up a different liability scheme for copyright-related takedown requests. The Network Act's liability scheme affects only takedown requests related to defamation, privacy, interference with business, etc. Although the Network Act's liability scheme on its face covers copyright as well, the Copyright

[36] Supreme Court, 2008Da53812, Apr. 16, 2009 (S. Kor.)..
[37] Section 512(c)(1)(A)(ii), 512(d)(1)(A).
[38] Park, Ahran. "Internet Service Provider's Liability for Defamation: South Korea's Balancing of Free Speech with Reputation" *Paper presented at the annual meeting of the Association for Education in Journalism and Mass Communication, The Denver Sheraton, Denver, CO*, Aug 04

Act's scheme takes precedence in copyright issues in accordance with the principle of *generalia specialibus non derogant*. Although there will be issues with copyright-related on-demand takedowns, the Copyright Act's liability scheme was quite similar to the American DMCA and is now more so under the KORUS FTA-triggered amendment that closed the final loophole by making the liability exemption mandatory.

There is nothing similar to the Transparency Reports of U.S. OSP's that are published by Korean intermediaries. There are only statistics occasionally obtained through private sources along with legislators who exercise their clout with agencies, which can in turn make various disclosure demands to the intermediaries licensed or registered with them. MP Choi Moon-Soon obtained the relevant data from the top three top content host intermediaries though the Korea Communications Commission and made the following disclosure in November 2010.[39]

Operators Years	Naver	Daum	NATE	**Total**
2008	31,953	27,454	691	**60,098**
2009	37,342	57,712	1,449	**96,503**
2010 up to September (estimated year-end figures)	27,914 (37,125)	45,798 (60,911)	956 (1274)	**74,668** **(99,310)**

Figure 2. *Non-copyright related takedowns pursuant to Article 44-2*

After learning that the number of takedowns executed by the top two content hosts exceeded that of other hosts greatly, MP Nam Kyung-pil obtained similar data on the two content hosts in October 2012,[40] shown below.

Operators Years	Naver	Daum
2008	70,401	21,546
2009	83,548	50,860
2010	85,573	58,168
2011	123,079	86,431

[39] http://moonsoonc.tistory.com/attachment/cfile23.uf@133D7F0F4CE1EF660D3B87.hwp
[40] "Temporary Measures Presented - No Clear Criteria Strengthened." *Match eTV News*. Accessed February 17, 2015. http://www.ggetv.co.kr/news/articleView.html?idxno=16781.

2012 until July	104,578	40,538

Figure 3. *Non-copyright related takedowns pursuant to Article 44-2*

Although the differences in the two tables need some explanations,[41] the following facts are uncontested:

- The number of URL takedowns privately requested under Article 44-2 of the Network Act for non-copyright purposes has increased over time.
- The annual number of URLs taken down by Naver hovers above 100,000 and for Daum is about 50-70% of Navers' number.

How serious is this? There is nothing here that we can compare to the situation in the U.S. because Section 230 of CDA insulates the intermediaries from liability for defamation and other non-copyright related laws. However, we can compare these Korean numbers to government-originating takedowns in other countries. Google received only about 4,000 takedown requests in 2012 from the whole world, only about half of which Google complied with.[42] So, 100,000 in Korea vs. 2,000 the whole world vis-à-vis Google! As another example, the Korean government's censorship body – the Korean Communication Standards Commission – issued 54,385 takedown requests to various intermediaries in 2011, out of which only 668 were related to defamation and other rights infringement.[43] Although the number of URLs is usually greater than the number of requests – for each request may cover more than one URL – the rights-infringement category of KCSC activities usually covers less than 10 URLs. This means that private censorship takedowns through Article 44-2 is more than 10 times the number of rights-infringement takedowns executed by the Korean government.

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

- A posting[44] critical of a Seoul City mayor's ban on assemblies in the Seoul Square;
- A posting[45] critical of a legislator's drinking habits and introducing his social media account;
- Clips of a television news report on the Seoul Police Chief's brother who allegedly runs an illegal brothel-hotel;[46]
- A posting critical of politicians' pejorative remarks on the recent deaths of squatters

[41] Naver's numbers in the first table represent the number of requests, which can cover more than one URL, while the Naver numbers in the second table represent the number of URLs taken down. Daum's numbers in the first table include both permanent removals and temporary measures, i.e., blinds while Daum's numbers in the second include only temporary measures. Daum's numbers in the second table more and more came to represent the total number of takedowns as Daum cancelled its policy of undoing the blinds after 30 days, i.e., all temporary measures became permanent.

[42] "Government Requests to Remove Content." https://www.google.com/transparencyreport/removals/government/.

[43] https://www.kocsc.or.kr/02_infoCenter/info_Communition_View.php?ko_board=info_Communition&ba_id=4909

[44] http://blog.ohmynews.com/savenature/199381

[45] The original posting now taken down is shown here. http://wnsgud313.tistory.com/156

[46] "Police Arbitrarily Issue 'Defamation Judgement'. Even Foreign Carriers Face Censorshop." Accessed February 17, 2015. http://www.hani.co.kr/arti/society/society_general/300688.html.

and police officers in a redevelopment dispute;[47]

- A posting calling for immunity from criminal prosecutions and civil damage suits on labor strikes;[48] and
- 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.[49]

V. 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 shield intermediaries from liability for even unlawful content. However, Korea does much worse: it chills the intermediaries into taking down even lawful content, as evidenced by the examples above. The PSPD Public Interest Law Center and others filed a constitutional challenge against Article 44-2 of the Network Act on the theory that the total result of the aforesaid provisions is that "Thou Shall Delay Saying What Others Dislike, As Long As 30 days."[50] The Korean Constitution does not authorize suppressing speech that does not violate others' rights, the aforesaid provisions de facto require even lawful content to be removed 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 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 requires even Naver to take down content that 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 challenges as follows:[51]

> "The instant provisions are purported to prevent indiscriminate circulation of the information defaming or infringing privacy and other rights of another, and therefore have a legitimate purpose . . .Temporary blocking of the circulation or diffusion of the information that has the possibility of such infringement is an appropriate means to accomplish the purpose…
>
> Freedom of speech requires absence of restriction in form, method, and timing of speech. Especially, in relation to publishing one's opinions on a certain issue or event, the 'temporal pertinence' i.e. making a remark appropriate to the event in a time proximately related to the subject of that opinion is an important component of free speech and should be maximally guaranteed. This is an important function of freedom of speech that calls for self-correction through rebuttal and discussions about that speech, conducted at 'the marketplace of ideas.' Therefore, the instant provisions' 'temporary measure' depriving

[47] http://blog.jinbo.net/gimche/?pid=668
[48] http://blog.jinbo.net/gimche/?pid=492
[49] http://bbs1.agora.media.daum.net/gaia/do/debate/read?bbsId=D115&articleId=610524
[50] Park Kyung-sin, "Unconstitutionality of Korea's Temporary Blinds on Internet - "Thou Shall Not Speak for 30 days What Others Do Not Like", Chung-Ang-Bub-Hak (Korean) <http://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART001387276>
[51] Constitutional Court 2012.5.31 Decision 2010 Hun-ma 88

> the speech of the temporal pertinence by blocking access through information communication network presents a grave restriction on free speech…
>
> However, . . .when another's personal rights such as privacy or reputation are infringed or are anticipated to be infringed, a need to temporarily block the infringing information is greater than the need to guarantee the temporal pertinence of the information. The fact that the content was disclosed may be further propagated through other means, and may cause privacy-infringement and defamation to an equal extent. In such situation, publishing a rebuttal by the infringement complainant, blocking of the links, search restrictions, expeditious dispute resolution, etc., cannot be effective alternatives to accomplish the legislative purpose…
>
> 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 . . ."

What was encouraging was that the Constitutional Court saw through to the practical effects of the provisions and recognized that the provisions are in fact tantamount to requiring the takedown of content that is not illegal. The Court itself states: "if the prerequisites are met, the service provider must without hesitation take the temporary measure."

However, the opinion takes a curious turn and rationalizes the blocking of content on the basis of the mere "anticipation" of infringement. 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 content that is lawful on that medium.

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

VI. Conclusion and Impact Assessment

The Korean liability regime starts out with an innocent-sounding rule that an intermediary shall remove any user-created content infringing on the rights of another. The regime adds yet another innocent-sounding rule that an intermediary is free to remove a UCC temporarily as long as the intermediary anticipates a dispute or faces difficulty in deciding on the lawfulness. Such a regime, exempting not posting but only the removal of a post, has caused in Korea rampant private censorship, and the removal a significant amount of content duly informative to the public on civic affairs. The courts have not behaved better, imposing liabilities on the

intermediaries for not taking down unknown content for which a takedown request did not even exist. Civil society has responded with a constitutional challenge, which ended with a surprising decision by the Constitutional Court that the Internet, due to its hyper-efficient mediating power, must be discriminated against so that even lawful content is subject to temporary removal if there are people who allege an injury.

Appendix D:
Brazilian Courts and the Internet – Rulings Before and After the Marco Civil on Intermediary Liability

NoC Online Intermediaries Case Studies Series: Brazilian Courts and the Internet – Rulings Before and After the Marco Civil on Intermediary Liability

Carlos Affonso Souza and Ronaldo Lemos,
Institute for Technology & Society

Editorial Note: Context, Character, and Purpose of the Case Study

This case study is part of a globally coordinated, independent academic research project by the Global Network of Interdisciplinary Internet & Society Research Centers (NoC). Facilitated by the Berkman Center for Internet & Society at Harvard University, the project is the first output of a larger policy-oriented research initiative that examines the rapidly changing landscape of online intermediary governance at the intersection of law, technology, norms, and markets. In concert with other research projects, it seeks to develop criteria, comparative methods, and a shared data repository, and to compile insights and lessons learned across diverse communities of knowledge aimed at informing and improving Internet policy-making globally.

The initial research output consists of a case study series exploring online intermediary liability frameworks and issues in Brazil, the European Union, India, South Korea, the United States, Thailand, Turkey, and Vietnam, and a synthesis paper that seeks to distill key observations and provide a high-level analysis of some of the structural elements that characterize varying governance frameworks, with a focus on intermediary liability regimes and their evolution.

The authors of these case studies have participated in a multi-step process of in-person consultations and remote collaborations among a global team of researchers from the Network of Centers. Additionally, the case studies are based on a set of broader questions regarding the role of online intermediaries in the digital age.[1]

The research effort is grounded in a diversity of global perspectives and collaborative research techniques, committed to objective and independent academic standards, and aspires to be useful, actionable, and timely for policymakers and stakeholders. More broadly, the Network of Centers seeks to contribute to a more generalized vision and longer-term strategy regarding the role of academic research, facilitation and convening, and education and communication in the Internet age. For additional information on the initiative, please contact Urs Gasser, Berkman Center for Internet & Society, at ugasser@cyber.law.harvard.edu

[1] The process is documented at: "Online Intermediaries: Functions, Values, and Governance Options", The Global Network of Internet & Society Research Centers, 2014 https://drive.google.com/file/d/0B_ToTBKP5ITVWTl0UzV0U3B2RlU/view?usp=sharing.

Abstract: This paper discusses the treatment of online intermediary liability by Brazilian Courts both before and after the establishment of the Marco Civil. It first provides an overview of the three most common approaches to intermediary liability applied by the Courts in the decades prior to the Marco Civil. The paper then describes the drafting and passage of the Marco Civil – "The Brazilian Internet Bill of Rights" – as well as the system of civil liability for online intermediaries established by this document. While the Marco Civil has both clarified the position of online intermediaries in Brazil in regards to third-party content and established more robust protections for these entities, it is still too early to tell what the full implications of the implementation of the Marco Civil will be for the Brazilian Internet landscape.

Table of Contents

I. Introduction

The Internet is a network that fosters freedoms, yet at the same time allows unprecedented control over individuals. It is an extraordinary platform for freedom of expression and – perhaps for the very same reason – can generate large-scale damage to one's reputation and privacy.

This multitude of paradoxes guides the way to a deeper understanding of the dilemmas that must be addressed in order to reach a balance between the various interests of companies involved in the provision of access to the internet, and others services throughout this network.

Who is liable for damages caused online? The individual who posts a photo, a video, or a text that damages others, or the provider that, through its own activities, may provide the platform for that offense to occur?

This report focus on the current state of this discussion in Brazil, analyzing solutions created by a decade of judicial decisions on the topic of online intermediaries' liability and the newly established regulatory framework as set forth in the so-called Marco Civil.

II. Who is the Provider?

Before exploring the debate around the framework for the civil liability regime for online intermediaries, it is necessary to identify exactly who an intermediary is in the Brazilian context.

Several authors have suggested different categories to identify intermediaries based on the activities they undertake. The Brazilian Superior Court of Justice (STJ), in assessing frequent cases involving damage over the Internet, has adopted the following classification:

> "*Internet service providers* are those that offer several services related to the operation of the network. There are several categories of Internet service providers: (i) backbone providers, which hold the infrastructure capable of processing large volumes of information. They are responsible for Internet connectivity, offering its infrastructure to third parties, which end up contracting with end users to allow access to the network; (ii) access providers, which acquire access to the infrastructure through backbone providers and resell to end users, enabling them to have access to the Internet; (iii) hosting providers, responsible for the storage of third party's data, allowing them remote access to it; (iv) information providers, which actually create the information available on the Internet; and (v) content providers, who make available the information created by information providers or by Internet users."[2]

Law No. 12965/2014 (known as "Marco Civil da Internet", or simply "Marco Civil"), deals in particular with two types of intermediaries: those dedicated to providing Internet access ("connection providers" or "access providers") and those that provide the most diverse services to the network ("application providers"). Article 5 of this Law defines the activities performed by each of these providers.

> Article 5. For the purposes of this Act, the following concepts apply:

[2] STJ, Resp no. 1316921/RJ, Justice Nancy Andrighi; 26.06.12.

V - Internet connection: the enabling of a terminal for sending and receiving data packets over the Internet through the assigning or authentication of an IP address; (...)

VII - Internet applications: the set of functionalities that can be accessed through a terminal connected to the Internet.

Understanding which activities the providers and their respective technical features perform is paramount to assessing the corresponding liability regime. In this regard, it is especially relevant to analyze the activities developed by their users and the extent to which the intermediary intervenes in these activities.

The question is thus how to create a liability regime that – on the one hand – does not harm the victim of any damage sustained online though the perpetuation of the illicit content, but which also does not encourage the intermediary to simply remove the photo, video, or text as soon as a notification is received, thus affecting the freedom of expression and diversity of online speech.

Is it up to the intermediary to judge the legality of the content displayed and to decide on its maintenance or removal? How do these questions impact the degree of innovation and future business models that may be affected by the way in which the law encourages prevention and imposes liabilities for damages caused online?

III. Brazilian Case Law on Liability of Online Intermediaries

After a decade of judicial decisions on the liability of online intermediaries in Brazil, one of three understandings were typically applied by national Courts. The first understanding exempts the provider from any liability for a third party's behavior. The second enforces a strict liability regime for the Internet providers, grounded in the concept of the risk of the activity or in the recognition that a service was defectively rendered. A third and final understanding would link the liability of the provider to the existence of fault on its part. Some consider the provider liable simply for the non-removal of the content after the provider becomes aware of its existence (usually through a notification sent by the victim), while some understand liability as arising from non-compliance with a Court decision ordering the removal of the offending material. The latter was the understanding adopted in the recently enacted Marco Civil.

More than simply categorizing the understandings shared by national Courts, it is necessary to understand what the grounds are for supporting each position adopted by the Courts and which factual circumstances may have been relevant for the outcome of these decisions.

A. The Provider Is Not Liable for the Conduct of Its Users

The first understanding – according to which the provider would not be held liable for the acts of its users – is frequent in cases that identify the provider as a mere intermediary between the user (the offender) and the victim. In general there would be no conduct by the provider that would make it responsible for the acts of others. The provider's only responsibility would be to help identify the offender.

In the majority of judicial decisions enforcing this understanding, it was very clear that the intermediary, in providing a specific service, was already informed that it would not be held

responsible for content generated by its users, whether they are members of a social network or users of a webhosting platform.

In the beginning of the last decade, some Courts adopted this understanding, usually excluding the provider as a possible defendant in compensation claims filed by the victims of damages caused by users of the intermediary.

The Court of Appeals of the State of Paraná, analyzing a case involving offenses to the reputation of a victim made available on a website hosted by the intermediary, stated that:

> "In the hosting agreement, the provider is only responsible for making an online space available. It must not interfere with the content that is published, except in cases of notorious illegality. The current Brazilian legal system does not allow the liability of the hosting provider, either strict or jointly, for moral damages arising out from the insertion of offensive material by the subscriber."[3]

Around the same period, a case involving a couple of lawsuits brought by former soccer player Paulo Roberto Falcão against Terra (an access and application provider) received some press coverage. The lawsuits claimed damages for offensive material that have been published on the website of the "Isto É Gente" magazine, hosted by Terra. The Court of Appeals of the State of Rio Grande do Sul recognized that the hosting provider could not be sued for the contents of a webpage that it simply hosts.[4]

B. Strict Liability

The application of a strict liability regime for Internet providers is usually grounded in the notion of risk or defect in rendering a service to consumers.

Regardless of the grounds adopted for its enforcement, the use of such an understanding in national case law leads to two relevant concerns.

First, does the provider have the duty to inspect, monitor, and consequently filter out content that is submitted by its users? That would be the very first concern, since the discussion around the duty of monitoring is key to understanding the effects of strict liability for providers. In this sense, the provider could be held liable for the mere display of harmful content (either because it is an inherent risk of their activity, or because there were a defect in the rendered service).

Second, should the provider be liable if, once aware of the reputedly harmful content – usually when notified by the victim – it does not remove it? This second concern takes into account the fact that providers should not be held liable for simply making the content available, but rather for the decision (active or passive) to not remove the challenged material.

Analyzing the first concern, it is relevant to highlight how the concept of risk has been applied in national case law. The large amount of lawsuits over damages caused online, especially focused

[3] TJPR, Civil Appeal nr. 130075-8, 19.11.2002.
[4] TJRS, Agravo de instrumento nr. 70003035078, Judge Paulo Antonio Kretzmann, 22.11.2001

on the use of social networks,[5] has drawn attention from the Judiciary due to the frequency in which such services are used to infringe third parties' rights.

At the same time that access to the Internet in Brazil began to be widespread in the last decade, a new Civil Code was approved in 2002, providing for – in article 927 – strict liability for those who develop activities that, by their nature, involve risk to third party's rights.

Therefore, as the number of cases brought to Court grew in the last decade, case law ended up establishing the understanding that a number of agents – from companies that operate search engines to owners of Internet cafes – could be held liable for the risk assumed in the development of their respective activities.

The Court of the State of São Paulo decided, in a lawsuit filed by the victim of defamatory messages sent our from an Internet café that the owner of such establishment should be liable as per "(...) the strict liability clause provided for in article 927, sole paragraph, of the Civil Code, as the development of its activity involves risk to the rights of others. (…) In this sense, whoever provides computer terminals or wireless network for Internet usage assumes the risk of misuse of the system to infringe third party's rights, as it have happened in the present case."[6]

In opposition to such an understanding, a number of scholars sought to investigate not only whether there is risk in the activity, present in everyday situations, but also whether the risk posed by the activity performed by the intermediary is greater than usual. In this regard, the strict liability provision should only be applicable in extraordinary cases. As Erica Barbagalo explains:

> "We understand that the activities undertaken by service providers on the Internet are not risk activities by their very nature, involving risks to rights greater than the one of any other commercial activity. Interpreting the law in the sense that any damage should be compensated regardless of culpability element would definitely burden the productive activities and therefore hinder development."[7]

The strict liability understanding based on the notion of risk was a minority view in the Court system by the end of the decade. The STJ, on several occasions, rejected this understanding. As stated in Special Appeal nr. 1308830/RS:

> "The material damage resulting from messages with offensive content on the site uploaded by users does not constitute risk inherent to the activity of content providers, so that it does not apply to them the strict liability regime provided for in art. 927, sole paragraph, of the Civil Code."[8]

A second ground for the liability of the providers then lies in the characterization of the legal relationship between the victim and the intermediary as a true consumer relationship, which

[5] In May 2012, Justice Nancy Andrighi mentioned that around 200 lawsuits involving Google alone were pending decision in the STJ (STJ, Resp 1308830/RS, Justice Nancy Andrighi; 08.05.2012).
[6] TJSP, Process nr. 583.00.2006.243439-5, Judge Ulysses de Oliveira Gonçalves Junior; 06.03.2008.
[7] Erica B. Barbagalo. "Aspectos da Responsabilidade Civil", in Ronaldo Lemos, Ivo Waisberg (orgs) Conflito de Nomes de Domínio e Outras Questões Jurídicas da Internet. São Paulo: RT, 2003; p. 361. See also STJ, Resp 1067738/GO, Justice Sidnei Beneti, 26.05.2009.
[8] STJ, Resp 1308830, Justice Nancy Andrighi; 08.05.2012. See also STJ, RESP 1306066/MT, Justice Sidnei Beneti; 17.04.2012.

therefore results in application of the strict liability regime under the Consumer's Protection Code (CDC).

After some debate in the late nineties on the enforcement of the CDC for online activities, it is worth noting that the main argument initially presented by providers when attempting to avoid liability was the non-essential nature of the service they were rendering.

Although a large numbers of services are rendered through the Internet without charging a specific value, national Courts decided that there is a counterpart offered by the consumer, even if it is of indirect nature. According to such case law, instead of paying a certain amount of money to the provider, this entity it earns profits from its users in other ways, especially through the creation of a user's profile, which contains personal information and browsing habits, and can be used to generate advertising revenues through customized marketing based on the user's data.

As explained by Professor Claudia Lima Marques:

> "The expression used by art. 3 of the Consumer Protection Code include all consumer services rendered in connection to a 'remuneration' of some sort. (...) It seems to me that the choice of the expression 'paid' creates an important opportunity to include consumer services paid indirectly, ie, when it is not the individual consumer who pays, but the collectivity or when he/she pays indirectly. The term 'compensation' allows you to add all those contracts in which it is possible to identify the hidden synallagma (hidden counterpart), an indirect remuneration for the service rendered to the consumer." [9]

The subject was addressed a number of times in Superior Court of Justice decisions. In one of the first cases to reach the STJ on the liability of Internet service providers, the Court stated that, "to characterize the consumer relationship, the service can be provided by the provider for remuneration obtained indirectly." [10]

More recently, the STJ reinforced this understanding, thus confirming the enforcement of the CDC in the relationship between the provider of a social network and the victim of offenses made available in a community created on Orkut:

> "Commercial use of the Internet is subjected to the regulation of consumer relations arising out from Law No. 8.078/90. 2. The fact that the service provided by the Internet service provider is to be free does not change the nature of the relationship as a consumer one, since the term remuneration, contained in art. 3, §2, of the CDC, should be interpreted broadly so as to include the indirect gain from the provider."[11]

Once the relationship is subsumed under the Consumer Protection Code, it remains to ascertain whether the damage caused by the service can be framed as a defect in the service. The question of risk appears again to reveal the importance of the first concern mentioned above: if the provider has a duty to monitor the content that is made available on its pages, the mere display of harmful content implies a defect in the service rendered.

---

[9] In Comentários ao Código de Defesa do Consumidor. São Paulo: Revista dos Tribunais, 2003; p. 94.
[10] STJ, Resp 566468/RJ, Justice Jorge Scartezzini, 23.11.2004.
[11] STJ, Resp 1308830/RS, Justice Nancy Andrighi; 08.05.2012.

The STJ has already decided on several occasions that the service provider has no obligation to monitor the content of text, photos, videos, and codes entered by its users. As stated in the Special Appeal nr. 1308830/RS:

> "A prior inspection on the content of the information posted on the web for each user by the content provider is not intrinsic to the service, so it can not be deemed a defective activity under article 14 of the CDC, if the site does not examine and filter the data and images uploaded by its users."[12]

Another opposing argument to the imposition of surveillance duties (and consequently to the strict liability understanding) is the assertion that, by requiring the inspection of the posted contents, a censorship regime would be implemented, hindering freedom of expression.

This argument is represented by the Republic's General Attorney in a currently ongoing case to be decided by the Supreme Court (STF) involving the creation of a community in the Orkut social network that was reputedly offensive. The community "I hate Aliandra" ("Eu odeio a Aliandra") was created to mock a high school teacher in the State of Minas Gerais. The teacher then filed a suit against Google for the damages caused by this content.

The lawsuit questions if the providers should monitor what is said in the community pages created on social networking sites as a way to prevent future damage. According to General Attorney:

> "...There is no interference from the provider in the content posted by users on the social networks, being incompatible with the constitutional framework to allow or even to require previous censorship of disseminated manifestations, under penalty of strict liability. It would amount to undue and severe embarrassment to the very freedom of expression."[13]

The STJ, in support of this view, has even claimed that, "prior editorial control of the content of the information equates to a breach of confidentiality of correspondence and communications, prohibited by Art. 5, XII, of the Constitution."[14]

The understanding of the STJ of service providers in general needs to be analyzed carefully because, on one hand, the Court recognizes that such relationships are subject to the Consumer Protection Code but, on the other, it does not impose a strict liability (as it would be the rule in the CDC).

If there is a negative answer to the first concern raised (i.e. that "providers have no duty to monitor and are not liable simply by making a content available"), then there is a need to examine the second, which require an investigation regarding whether the provider would be liable if it fails to remove the infringing content once it has become aware of its existence.[15]

---

[12] STJ, Resp 1308830/RS, Justice Nancy Andrighi; 08.05.2012. See also STJ, Resp 1316921/RJ, Justice Nancy Andrighi; 26.06.2012.
[13] Manifestação da Procuradoria Geral da República, RE nr. 660861/MG, 11.07.2012.
[14] STJ, Resp 1308830/RS, Justice Nancy Andrighi; 08.05.2012.
[15] See STJ, Resp 997993/MG, Justice Luis Felipe Salomão; 21.06.2012.

C. Fault-Based Liability

The third understanding of intermediary liability is based on the existence of a fault by the provider, attaching to itself the responsibility for the conduct performed by its user. This understanding has two different grounds for application: the first states that the liability should result from noncompliance with a notification informing the provider of the infringing material; the second is based on noncompliance with a Court order requesting the removal of certain material. This last understanding is the one adopted by the Marco Civil.

In its most recent decisions on the issue, the STJ affirmed the understanding that Internet service providers can be liable when they fail to remove illegal content of which they are aware by a notification sent by the victim. Such an understanding has been enforced for both cases in which the provider fails to respond to the notification of the victim, or actively responds to the notification stating that it sees no reason to remove the content. In such cases, the responsibility would be based on fault and jointly affirmed with the liability of the user that has directly uploaded the infringing material.

On this topic it is worth mentioning some relevant excerpts from Special Appeal nr. 1.193.764/SP, as decided by the STJ:

> "By offering a service through which it allows users to freely express their opinions, the content provider should take care to provide resources so that it can identify those users, curbing anonymity and assigning each event a certain authorship. From the perspective of the average diligence expected of the provider, it must adopt the measures which, according to the specific circumstances of each case, can individualize the website's users, under penalty of being liable for fault (*culpa in omittend*)."[16]

This debate was also reported in the decision of the STJ in the Regimental Appeal presented in the Special Appeal nr. 1.309.891/MG. In this case there is a deeper discussion over the expression "immediate" as to how quickly the provider should act to remove the infringing content:

> "In line with precedents of this Court, the Internet content provider is not liable according to a strict liability regime for the content created by the user in a website, as this is not an inherent risk to their activity. It is required, however, to immediately takedown the morally offensive content, otherwise it would be jointly responsible with the direct offender. Precedents.
>
> In the present case the Court held that there was no immediate exclusion of the fake profile because the victim, for more than once denounced the illegality perpetrated by electronic means provided for this purpose by the provider itself, without obtaining any result.
>
> Regimental Appeal dismissed."[17]

The case above, as decided by the STJ, verified the decision of lower level Court that found Google – when exploring the social network Orkut – was not diligent in promoting the removal

[16] STJ, Resp 1193764/SP, Justice Nany Andrighi; 14.12.2010.
[17] STJ, Agr. Reg. in Resp 1309891/MG, Justice Sidnei Beneti; 26.06.2012.

of offensive material as it took eleven days to remove the content. Cases like this call into question the frequent use of the expressions "immediately" or even "energetic" by the STJ when it comes to damages caused through online intermediaries.

1. General Effects of a Notice and Takedown Regime

The liability of the provider for not removing the content once notified seems intuitive: if the provider is aware that someone claims to be suffering damages due to a content made available by your user, the one who stands in the best condition to cease the damages – other than the offender himself – would be the provider. However, this hides many harmful consequences for the operations of the Internet and for the protection of many fundamental rights.

At first one must question whether the provider should promptly remove the content and thus prevent the ongoing damage. Would it be appropriate for the provider to analyze whether the content is or isn't actually infringing? The danger of this alternative lies in empowering providers to decide what should and what should not be made available on criteria that go beyond those presented in their terms of service.

The STJ has had the opportunity to express some concerns with this broad delegation of the power to control speech online to private actors. As mentioned by Justice Nancy Andrighi:

> "We must consider the impossibility to define a criteria that would authorize the veto or the disposal of given page. Given the subjectivity surrounding the psychological damage and/or the damage to one's image, it would be impossible to define parameters that could allow the providers to rely on to define whether a content is potentially offensive. On the other hand, it would be reckless to delegate this judgment to the discretion of the providers."[18]

The second point worth mentioning is precisely the intense subjectivity of the criteria that can be used to allow content to be removed. If it does not make sense to hold the providers liable just because content was made available and there is doubt on whether it is infringing or not, then a system that lacks transparency and that is highly subjective, removing content and jeopardizing the diversity and the degree of innovation on the Internet, should undoubtedly be rejected.

The degree of innovation on the Internet is the third point that can be mentioned in opposition to a system of fault-based liability arising out from the failure to remove content after being notified. The development of all new activity involves questioning its adherence to the current legal regime and, in most cases, an investigation into potential judicial decisions on the subject. The removal of content in a very subjective way and by a mere notification creates serious obstacles to the development of new alternatives for exploration and communication on the Internet, dampened by fear of future claims that could be filed if notifications requiring the removal of contents are not "immediately" complied with.

A fourth important point relates to judicial analysis of cases that could provide greater legal certainty for business developed on the Internet. If, for fear of liability, providers end up taking down massive amounts of content, the immediate result is a reduction in the number of cases on which the Judiciary could act to draw the limits of expression in the Internet. This could relegate

[18] STJ, Resp 1316921/RJ, Justice Nancy Andrighi; 26.06.2012.

the establishment of mechanism for content removal to private parties, resulting in processes that might not be in accordance with judicial standards for expression in other media, for instance.

A notice and takedown regime that renders the provider liable for not taking down certain content after being notified creates two alternatives equally detrimental to the diversity of the discourse on the network. Either the provider takes down the content as soon as it receives the notification and thus gives rise to the whole range of abuses stemming from the ease of removing content that may be harmful to others (with strong impact on freedom of speech, of press), or the provider fights to maintain the content online, understanding that it has no reason to be removed and thus assuming the risk of being held legally responsible for that very content. This situation creates little incentive to protect freedom of expression for all providers and creates a strong disincentive for small providers that cannot bear the burden of mass litigation.

Therefore, even if the application of liability based on fault offers superior results to that obtained by imposing strict liability, one must realize that to affirm liability arising from the failure to comply with a notification has a number of negative implications for the way in which the Internet operates. Thus, this system needs to give way to liability rooted in compliance with Court decisions, such as that provided by the Marco Civil.

D. The Special Case of "Search Providers"

Before dealing with the liability regime provided by the Marco Civil itself, it is worth noting that the Superior Court of Justice (STJ) has given different treatment with regards to liability to so-called "search providers" than to other services and applications, such as social networking and webhosting. According to recent decisions by the STJ, when acting as a simple search engine Google will not be held liable for the content displayed as search results.

The most famous case that affirms this understanding is a case involving the actress and TV host Xuxa Meneghel, which sought to compel Google to remove from the engine all results for the search term “pedophile xuxa” or even other result involving the name of the Plaintiff, partially or fully written, regardless of spelling, in connection to any criminal act."[19]

The motivation for the lawsuit was the widespread availability on the Internet of an early 80s movie called “Love Strange Love” (“Amor Estranho Amor”),[20] in which the actress is featured in two scenes having intimate relations with a 12-year old boy. Much of the actress’ concern is due to the fact that, shortly after the movie was released, she began a career on TV hosting a show focused on kids and teenagers. The availability of such material online could hamper the image she has created in recent decades.

The STJ decided in favor of Google in this lawsuit. The decision is grounded in the relevance of search providers (part of the “application providers” category, in the language of Law nr. 12695/14) in indexing the information found on the Internet. According to the leading vote of Justice Nancy Andrighi:

> “Search providers perform their searches within a virtual universe, whose access is public and unrestricted, ie, its role is limited to the identification of web pages where certain

[19] STJ, Resp 1316921/RJ, Justice Nancy Andrighi; 26.06.12
[20] http://en.wikipedia.org/wiki/Love_Strange_Love

> data or information, even if illegal, are being freely made available. Thus, although the search engine facilitate access and the consequent dissemination of pages whose content is potentially illegal, these pages are public as parts of the world wide web and therefore appear as results of the research sites."[21]

As a consequence of the role played by search providers on the Internet, they can not be required to overturn the indexing mechanism for addressing third parties' pages; this would unduly interfere with the legitimate collective interests, such as access to information. According to the judgment:

> "Search providers should not be required to remove from their system the results derived from the search term or expression, nor the results that point to a specific photo or text, regardless of the indication of the URL of the page where it is inserted.
>
> It is not advisable, for the purposes of hindering the spread of illegal or offensive content on the web, to suppress the right to information. Balancing the rights involved and the potential risk of violation of each of them, the odds should favor the guarantee of freedom of information, as set forth in Art. 220, § 1, of the Constitution, especially considering that the Internet is today an important vehicle of mass media."[22]

Therefore, the decision from STJ indicates that the victim should seek to prosecute whoever is responsible for the damage, such as the person who actually published the illegal content, and refrain from prosecuting the search provider that only indexes the information freely found on the web.

> "If the conditions for the exclusion of a certain webpage are found, under the allegation of unlawful or offensive content - notably the identification of the URL of this page - the victim will lack interest to act against the search provider. If the victim identified though the URL the author of the illegal act, it has no reason to sue the one who merely facilitates access to this act, which has been so far publicly available on the network."[23]

Two comments seem especially relevant on cases involving search providers in the STJ. The first concerns to the difference in treatment accorded to the search engines compared to the liability regime typically adopted for social networks and video hosting sites. There are Court decisions that not only require providers to indemnify the content, but which also require these intermediaries to remove content in accordance with specific instructions from the Plaintiffs, creating a permanent channel for the exclusion of content based on the requirements authorized by the Court when a request is made.

The STJ, in tackling the case of the search provider, explicitly rejected this possibility, as mentioned in the previous judgment by the Court of Appeals of the State of Rio de Janeiro (TJRJ). As the vote of Justice Nancy Andrighi details:

> "Finally, it is important to assess the feasibility of the solution adopted by TJRJ, creating a process for removal of a certain content, previously indicated by the victim.

[21] STJ, Resp 1316921/RJ, Justice Nancy Andrighi; 26.06.2012.
[22] STJ, Resp 1316921/RJ, Justice Nancy Andrighi; 26.06.2012.
[23] STJ, Resp 1316921/RJ, Justice Nancy Andrighi; 26.06.2012.

> This form of restriction, if applicable, should always arise out from a judicial order, as it would be impossible for a simple extrajudicial notification to achieve such result. To have this process conducted through private notifications would end up delegating the judgment about the offensive potential of a given text or image to the discretion of the victim or the provider.
>
> At the same time, there are precedents from this Court involving similar cases - liability for the content of offensive messages on social networks – in which we have decided, in general terms, that "once notified that a certain text or image is unlawful, the provider must act energetically to remove the material immediately. Failing to do so would render the provider jointly liable with the direct offender" (Resp 1.186.616/MG, DJE 31.08.2011. In the same direction, see: REsp 1.193.764/SP, DJE of 08.08.2011).
>
> In the specific case of social networks, the intermediary itself provides a system for complaints on its own platform, allowing users to report unlawful or offensive content. The respective term of use gives the provider the right to remove any page or content that is in breach of the Term of Service.
>
> Therefore there is a special agreement, which authorizes the provider to exercise a discretionary judgment, a circumstance that is absent in search engines. The use of such applications does not even require registration. It is essential, therefore, that the request for exclusion from the search results of a particular text or image is made in Court. "[24]

The second comment relates to the targeting by the victim of a specific search provider, instead of others that could be used to find the exact same content. In this case, the market share of Google results in a situation in which the company finds itself as the defendant in the overwhelming majority of the lawsuits against search providers.

This dilemma is no stranger to the STJ. Recent decisions highlighted the paradox and limitations of civil liability regimes when applied to the Internet. According to the vote of Justice Nancy Andrighi in Special Appeal No 1407271/SP:

> "...It must be noticed that [the victim] acted exclusively against Google when the video can be found through the use of several other search engines. Consulting CADÊ and BING sites, for example, held by MICROSOFT and YAHOO companies respectively, we have been able to find more than 100,000 results for the same term."[25]

Would the victim then be obliged to file a suit against all, or at least against the most relevant search providers to show the seriousness of his/her complaints? If this seems a strange requirement to protect one's rights to reputation, image, and privacy, it shows how lawsuits against search providers may not serve the best interest of the victim. It is increasingly difficult to achieve the total removal of harmful material, especially in the current stage of technological progress, with the constant emergence of new ways to share pictures, videos, and text from mobile devices and the large availability of ways to play, download, store, and encrypt content.

[24] STJ, Resp 1316921/RJ, Justice Nancy Andrighi; 26.06.2012.
[25] STJ, Resp 1407271/SP, Justice Nancy Andrighi; 21.11.2013.

IV. The Civil Liability of Online Intermediaries in the Marco Civil

Law nr. 12965/2014 seeks to establish "principles, guarantees, rights and obligations for the use of the Internet in Brazil" according to its first article. This Law is the result of a pioneer initiative, led by the Brazilian government, to use the Internet as a pool for consultation on the actual content of forthcoming legislation. Even before arriving in the National Congress, during the online debate phase of the initiative the issue of intermediary liability was one of the most debated topics, along with net neutrality and data protection.

The so-called Marco Civil (or "Brazilian Internet Bill of Rights") was the first experience in Brazil with the use the Internet as a way to broaden the discussion of a Draft Bill of Law, ensuring that a much more significant number of participants could get involved in the debate of the legislation.

Specifically concerning the civil liability regime for intermediaries, Law nr. 12965/14 provides two different treatments depending whether the intermediary falls into the category of connection/access provider or application provider.

A. Access Providers

Holding the access provider liable for the acts of its users is a practice that has been rejected by national and international Courts since the late nineties.[26] There are two common arguments for recognizing the non-liability of connection providers for the damages caused by third parties that are simply using their services to connect to the Internet.

The first argument lies in the technical impossibility on the part of providers to avoid harmful behavior by its users. It is noteworthy that this preventive conduct by connection providers is not only impossible but also undesirable, since it would lead inevitably to an increase in mass surveillance practices of controversial legality.

The second argument transcends the technological aspect by focusing on the rupture of any nexus ("nexo causal") between the damage caused to a third party and the act of simply providing network access to a user. The simple Internet connection does not seem to be the direct and immediate cause of the damage suffered by a victim, rather the damage is caused by the behavior specifically played out by the user that generated the illegal content.

Law nr. 12965/14 echoes such arguments in Article 18, as it exempts connection providers from liability for the actions of its users:

> Article 18. The provider of connection to Internet shall not be held liable for civil damages resulting from content generated by third parties.

It is important to mention that the exemption set forth in Article 18 only applies to cases in which the provider would be held liable for third party conduct. Connection providers are still liable for the damages they cause directly through their own activities, as shown by a large pool of cases decided in the national Courts. Among the cases involving the liability of connection providers

[26] See Religious Technology Center v. Netcom On-Line Communication Services, Inc, 21.11.1995. In Brazil, among many decisons, see: TJRS, Ap. Civ. n° 70001582444, Judge Antônio Correa Palmeiro da Fontoura, 29.05.2002.

are situations involving damage to their own users, such as the failure to provide services dully contracted by their users or in the different conditions than the ones previously established by either contract or the relevant sectoral regulations.

B. Application Providers

The liability of application providers is provided in the Article 19 of the Marco Civil in the following terms:

> Art. 19. In order to ensure freedom of expression and to prevent censorship, the provider of Internet applications can only be subject to civil liability for damages resulting from content generated by third parties if, after an specific Court order, it does not take any steps to, within the framework of their service and within the time stated in the order, make unavailable the content that was identified as being unlawful, unless otherwise provided by law.
>
> § 1. The referred Court order must include, under penalty of being null, clear identification of the specific content identified as infringing, allowing the unquestionable location of the material.
>
> § 2. The implementation of the provisions of this article for infringement of copyright or related rights is subject to a specific legal provision, which must respect freedom of speech and other guarantees provided for in art. 5º of the Federal Constitution.
>
> § 3. The compensation disputes for damages arising from content made available on the Internet related to the honor, reputation or personality rights, as well as the removal of related contents by Internet application providers, can be presented to special small causes Courts.
>
> § 4. The judge, including within the proceeding set forth in § 3º, can anticipate, partially or in full, the effects of the request contained in the initial petition, to the extent that undisputable proof exists of the fact, considering society's collective interest in the availability of the content on the Internet, as long as the requisites of truthiness of the author's claims, the reasonable concern of irreparable damage, or damage that is difficult to repair are met.

As previously mentioned, the Marco Civil affirms that the general rule for intermediary liability in Brazil is based on the fault of the provider, denying the attempts to hold them liable in typical strict liability standards, either by the simple availability of harmful content based on the risk theory or based on the rendering of a defective service.

At the same time that the Marco Civil evades strict liability, the approach it provides for liability based on fault is quite different from the usual liability arising out from the simple lack of action after being notified that damages are being caused by the availability a certain material.

Here lies perhaps one of the most heated controversies of the Law: the Marco Civil provides that intermediaries are only held liable if they fail to fulfill a Court order requesting the removal of content.

One of the most frequent criticisms of this provision is that the Marco Civil only allows content to be removed by a Court order. This is not the best interpretation of the mentioned provision.

What the Marco Civil sets forth is a safeguard for application providers in the sense that they will only be held liable if they do not comply with a Court order requesting the removal of the offensive material. This provision does not prevent intermediaries from determining their own requirements for removing content once notified by the alleged victims of damages arising out from materials made available through their platforms.

The Marco Civil gives freedom of expression high importance in this debate, guaranteeing to the providers an immunity that neutralizes any concern that they would have of being held liable for a lack of content removal once notified.

As mentioned by André Zonaro Giacchetta, analyzing the text while on debate in the National Congress:

> "The text of the Draft Bill clearly favors the guarantee of the rights of Internet users, instead of restricting their liberties. This is a standard created for the user in good faith. There is a clear choice for ensuring freedom of thought and expression, as well as the privacy of Internet users and the protection of personal data."[27]

Additionally, it is noteworthy that the solution provided by Law nr. 12965/14 does not necessarily oblige the victim to file a lawsuit in order to have the content removed. Such removal will depend on the terms of service of the website, the nature of the infringing content, the persuasive language of the notification in evidencing the damages caused by the same material and etc. However, the Marco Civil directs the settlement of any dispute between the victim and the provider to the Judiciary, as it recognizes Judiciary Power as precisely the legitimate authority to solve the controversy.

1. Judicialization and Its Effects

The Marco Civil fosters the understanding that an intermediary should not be compelled to remove content simply because a notification has been received. The provision of Article 19, as mentioned above, creates incentives for the claim to be brought to the Judiciary.[28]

One recurrent argument in this regard is the fact that the speed in which contents might be copied and shared through the Internet is not compatible with the time it takes for a lawsuit to be brought to the Judiciary. At the same time, it is important to stress that the Marco Civil expressly provides that a judge may order the removal by granting the victim an injunction in cases when it seems clear that the delay in taking the content down would worsen the victim's situation.[29]

In order to make this solution easier and faster for the victim of certain damages, the Marco Civil states that such cases can be brought to the Special Small Claims Courts. The provision in the

---

[27] André Zonaro Giacchetta. "A Responsabilidade Civil dos Provedores de Serviços de Internet e o Anteprojeto de Reforma da Lei n 9610/98 ("Lei de Direitos Autorais")", In Revista da Associação Brasileira da Propriedade Intelectual, n. 117 (mar-abr/2012); p. 39.

[28] See Marcelo Thompson. "The Insensitive Internet – Brazil and the Judicialization of Pain" (http://www.iposgoode.ca/wp-content/uploads/2010/05/Marcelo-Thompson-The-Insensitive-Internet-Final.pdf).

[29] See Marcel Leonardi. Responsabilidade Civil dos Provedores de Serviços na Internet. Brasília: Juarez de Oliveira; p.207.

third paragraph of Article 19 makes reference to cases of "compensation disputes for damages arising from content made available on the Internet related to the honor, reputation or personality rights, as well as the removal of related contents by Internet application providers."

The balance that the Marco Civil tries to achieve aims at accommodating all interests involved, protecting freedom of expression by clearly defining the role of the provider and ensuring that they must play a prominent role in the prevention and elimination of damage, while avoiding arbitrary judgments or fear of future liability.

If the situation is brought to a Court, the Marco Civil recognizes the Judiciary as the most appropriate forum for the resolution of such cases. At the same time, an interesting side effect of the Marco Civil is that it fosters capacity building of judges on the evolution of modern technologies for information and communication, as such knowledge is crucial to the exercise of their functions.

In affirming that application providers must only be held liable in cases in which fault is found, and not by simply failing to comply with a notification, the Marco Civil separates itself from the case law that has been created in the last decade in Brazil, especially by the Superior Court of Justice.

2. Two Exceptions to the Liability Regime

Law nr. 12965/14 has two important exceptions to the general liability regime, as described in the article 19: copyright infringement, as provided by the second paragraph of the article, and cases of so-called "revenge porn," provided by Article 21.

For both cases the general rule that intermediaries may only be held liable if they fail to comply with a Court order demanding the removal of the content is not applicable. These two situations, for very different reasons, can trigger the liability of the provider if it is notified and fails to remove a specific content.

i. Copyright

The exception concerning copyright was due to a continuous demand, especially by radio and television broadcasters, for the Marco Civil not to change the established practice of sending out notifications for the removal of copyrighted material made available without proper authorization or in circumstances not protected by the exceptions and limitations regime as set forth by the Copyright Act (Law 9.610/98). Brazilian Courts have recognized several times the liability of the application provider when, once notified, it fails to remove the content.

An additional circumstance that explains why such an exception was inserted in the review process of the original text of the Marco Civil in the National Congress was the fact that the Federal Government, through the Ministry of Culture, has been developing in recent years a process of consultations for the reform of the Copyright Act, dealing with topics such as liability for copyright infringements carried out online.

In this regard, the removal of further considerations on liability through copyright infringement would prevent the existence of two different regimes for the very same issue in Brazil: the one in the Marco Civil and the other as provided by an eventual reform of the Copyright Act.

It is worth noting that the Marco Civil has not simply deferred the treatment of such matters to the Copyright Act. The second paragraph of Article 19 of Law No. 12965/14 states that the regulation of online copyright infringement should be tackled by the Copyright Act, but at the same time it states that treatment under this Act should "respect freedom of speech and other guarantees provided for in Article 5 of the Federal Constitution."

The final part of this provision is quite revealing since one of the guidelines of the reform of the Copyright Act is to achieve a better balance between Copyright and other fundamental rights, such as access to knowledge and freedom of expression, and at the same time preventive abusive conduct in copyright enforcement. In this sense the Marco Civil advances some of the concerns of the Copyright Act reform, as envisioned by the Ministry of Culture, already providing an interpretive clause for whichever solution is adopted in the reform of the specific law.

ii. Revenge Porn

The second exception to the rule in Article 19 of the Marco Civil is the provision of Article 21 for cases of so-called "revenge porn"[30] materials.

The provision was inserted in one of the last rounds of editing on the text of the Bill and it was clearly motivated by the suicide of two Brazilian girls after intimate adult videos end up being shared through Whatsapp. A number of Congressmen have referred to this case as the trigger for creating an exception to the general rule on intermediaries' liability.

> Art. 21. The Internet application provider that makes third party generated content available shall be held liable for the breach of privacy arising from the disclosure of images, videos and other materials containing nudity or sexual activities of a private nature, without the authorization of the participants, when, after receipt of notice by the participant or his/hers legal representative, refrains from removing, in a diligent manner, within its own technical limitations, such content.
>
> Sole Paragraph. The notice set forth above must contain sufficient elements that allow the specific identification of the material said to violate the right to privacy of the participant-user and the confirmation of the legitimacy of the party presenting the request.

Article 21 creates a different liability regime from the general rule of Article 19 for the cases in which the application provider fails to remove materials that fall into the category presented above. It is important to highlight that the final part of the provision makes this exceptional liability conditional on evidence that the provider(s) have not acted in a *diligent manner*. This condition – together with the addition of the expression "within its own technical limitations" – could provide an opportunity for discussion in the forthcoming lawsuits on what the standards should be for how providers should act when they are given notice that intimate material, such as the ones targeted by this provision, has been made available through their applications.[31]

V. Conclusion

After more than a decade of case law on the liability of online intermediaries, the enactment of Law nr. 12965/14 tries to balance all relevant interests in the development of several online

[30] http://pt.wikipedia.org/wiki/Pornografia_de_vingan%C3%A7a.
[31] See STJ, Resp nº 1306157/SP, Justice Luis Felipe Salomão, 17.12.2013.

activities. The so-called “Marco Civil da Internet” has, since its origin, been intended to establish a human rights oriented perspective for the regulation of the Internet in Brazil.

Whether such balance has been achieved is a debate that still depends on how Brazilian Courts will interpret its provisions, enforce fundamental rights such as privacy, data protection, and freedom of expression, all in connection with the need to respect such rights and – at the same time – create a fruitful environment for innovation and development online.

Such an initiative is not entirely comprehended without knowledge of international and domestic politics around the negotiation of some of its most relevant provisions. In this case, the fallout from the Snowden revelations and a presidential election campaign had a great impact on how the text of the Marco Civil came to be.

In regards to the intermediary liability provisions, the addition of two exceptions – for copyright and revenge porn – during the last year of negotiations in the National Congress offers a glimpse of how different stakeholders have organized themselves for the protection of their respective interests in this piece of regulation.

As Brazil bridges the digital divide, the Marco Civil will serve as umbrella legislation, setting the principles for future regulation on matters concerning the Internet. As more and more people, especially from the peripheries of Brazil, connect to the network, it will be interesting to follow up on how practices and behaviors change.

The influx of Brazilian users in platforms intended for global usage, such as Google’s Orkut, has not only resulted in very innovative uses by Brazilians, but also a significant opportunity for balancing different interests in Internet regulation. The immense pool of judicial decisions on damages caused by Orkut’s users is a complex and not entirely explored body of research material.

Hopefully this report has covered the most relevant judicial decisions concerning online intermediary liability in Brazil and can serve as a guide to navigate the intriguing future of a country which, after a decade of debate, has finally enacted a human rights oriented piece of legislation that aims to promote the values that are inherent in the current stage of Internet development, while at the same time providing room for diversity and innovation.

Appendix E:
Online Intermediary Liability in Thailand

NoC Online Intermediaries Case Studies Series: Online Intermediary Liability in Thailand

Pirongrong Ramasoota
Thai Media Policy Centre, Faculty of Communication Arts, Chulalongkorn University

Editorial Note: Context, Character, and Purpose of the Case Study

This case study is part of a globally coordinated, independent academic research project by the Global Network of Interdisciplinary Internet & Society Research Centers (NoC). Facilitated by the Berkman Center for Internet & Society at Harvard University, the project is the first output of a larger policy-oriented research initiative that examines the rapidly changing landscape of online intermediary governance at the intersection of law, technology, norms, and markets. In concert with other research projects, it seeks to develop criteria, comparative methods, and a shared data repository, and to compile insights and lessons learned across diverse communities of knowledge aimed at informing and improving Internet policy-making globally.

The initial research output consists of a case study series exploring online intermediary liability frameworks and issues in Brazil, the European Union, India, South Korea, the United States, Thailand, Turkey, and Vietnam, and a synthesis paper that seeks to distill key observations and provide a high-level analysis of some of the structural elements that characterize varying governance frameworks, with a focus on intermediary liability regimes and their evolution.

The authors of these case studies have participated in a multi-step process of in-person consultations and remote collaborations among a global team of researchers from the Network of Centers. Additionally, the case studies are based on a set of broader questions regarding the role of online intermediaries in the digital age.[1]

The research effort is grounded in a diversity of global perspectives and collaborative research techniques, committed to objective and independent academic standards, and aspires to be useful, actionable, and timely for policymakers and stakeholders. More broadly, the Network of Centers seeks to contribute to a more generalized vision and longer-term strategy regarding the role of academic research, facilitation and convening, and education and communication in the Internet age. For additional information on the initiative, please contact Urs Gasser, Berkman Center for Internet & Society, at ugasser@cyber.law.harvard.edu

[1] The process is documented at: "Online Intermediaries: Functions, Values, and Governance Options", The Global Network of Internet & Society Research Centers, 2014 https://drive.google.com/file/d/0B_ToTBKP5ITVWTl0UzV0U3B2RlU/view?usp=sharing.

Abstract: This paper discusses the instability of the Thai government and society, and how this affects the implementation and creation of laws and policies relevant to online intermediaries. It addresses related laws and cases, along with primary survey data from online intermediaries. The 7-year-old computer crime law, the centerpiece of intermediary liability provisions, does not make the distinction between different types of intermediaries – those that deal directly with content as opposed to those that are merely conduits for content. Additionally, while only one case has been prosecuted so far in association with the controversial lèse majesté law, there has been a visible chilling effect on Internet operators as a result of this law, substantiated by primary research. Although most surveyed intermediaries tend to accept the burden imposed by the provision, some members of this group – together with online activists – are mobilizing in support of an amendment to the computer crime law, particularly with respect to the differentiation of types of intermediaries, the proportionality of penalties to the offence, and the tendency of government agencies to ask for "cooperation" from intermediaries in monitoring Internet content. Under the current interim government, which was installed under a military coup, intermediaries are compelled to carry out more censorship and surveillance, while also passing on more regulatory constraints to users than ever before.

Table of Contents

I. Introduction

Online intermediary liability is an emerging area for Internet studies in general and challenging terrain for research in Thailand, a country beset by chronic political instability and a media policy process uniquely rooted in the country's political and economic circumstances. To attempt to provide a comprehensive understanding of intermediary liability in such a setting, this paper will delve into the background context surrounding online intermediaries, review key intermediary liability provisions together with relevant legal experiences, and provide empirical data from a first-hand survey of how different groups of online intermediaries in Thailand are coping with the liability scheme, and the consequences thereof.

II. Background Context

This section explores the political context, social developments, regimes of Internet content regulation, and the nature of Internet control related to online intermediaries before and after the 2014 coup.

A. Political Context

Thailand is a country located in Southeast Asia, with a population of 67.44 million. Since 1932, the country has been governed by a constitutional monarchy. Democratic rule and general elections have been interspersed with military dictatorships and coups. The last coup, the sixteenth to date, was staged on May 22nd, 2014 by a military junta known as the National Council for Peace and Order (NCPO), following months of protests against the civilian government of the populist Pheu Thai Party due to allegations of corruption and attempts to pass an amnesty law[2] that would provide blanket protection for wrongdoers in past political conflicts.

Since November 2013, anti-government forces led by the so-called People Democratic Reform Committee (PDRC), composed of opposition politicians, urban elites, sympathizers of the palace, and conservative academics, as well as millions of supporters mainly from Bangkok and the Southern provinces, have staged rallies at major thoroughfares in the capital city, seizing the Government House and paralyzing many government offices. Their demand was the reform of Thai politics by removing the influence of the so-called Thaksin regime. Thaksin Shinawatra[3] is

[2] The final draft of the bill, passed by the House of Parliament at unusual hour (4 a.m.) on October 31, 2013, would have pardoned protesters involved in various incidents of political unrest since 2004, dismissed corruption convictions of powerful politicians and annulled the murder charges against past national leaders that might have been responsible for the deaths of protesters in anti-government rallies.

[3] Thaksin Shinawatra, founder of the deposed Thai Rak Thai (TRT) Party, was a famous telecommunications tycoon, having made his fortune from satellite and mobile phone concessions through his family business, Shin Corporation. Thaksin is also a popular political leader who led the longest democratic and civilian rule – six years – in contemporary Thai history. Thaksin's popularity was largely attributed to populist policies that featured income redistribution, cheap health care, microcredit schemes, and many policy innovations in support of globalization and neoliberal economy. However, he is not well liked by a large number of urban or middle-class voters who are repulsed by his arrogance, authoritarian tendencies, and policy discrepancy that benefit only his cronies. He was also widely accused of disloyalty to the crown, an accusation that was largely used as a justification for the September 19, 2006 coup. Even after he was deposed, Thaksin continued to be an influential figure in Thai politics. He reportedly masterminded several revolts including the red-shirt protest in 2010 which led to a House dissolution under then Prime Minister Abhisit Vejjajiva and a violent clash with the armed forces that led to more than 90 in casualties, both military and civilian.

a former Thai leader who was ousted in another coup in 2006. He is also the older brother of then Prime Minister Yingluck Shinawatra, who led the Pheu Thai Party to an election's victory in 2011 and had been running the country's administration ever since.

After sustained protests, Yingluck dissolved parliament in December 2013 and called an election. However, opposition MPs from the Democrat Party, which formed the core of the PDRC, led mass movements to boycott the elections, which were eventually nullified by the Election Commission on grounds of inadequate participation. Nevertheless, the protesters, led by the PDRC, vowed to continue demonstrating, claiming that her brother, ousted leader Thaksin Shinawatra, controlled the Yingluck government and that Yingluck lacked legitimacy to rule due to many charges of corruption. As a result of the House dissolution, the Yingluck administration became a caretaker government.

Meanwhile, Yingluck and members of the Cabinet were investigated by an anti-graft body and faced trial for a policy discrepancy related to the controversial rice mortgage scheme and abuse of power. In early May 2014, the Constitutional Court ruled that Yingluck had acted illegally when she transferred her national security chief, and ordered her and nine other cabinet members to step down, resulting in the Commerce Minister being reinstated as acting Prime Minister and creating a political void. Many viewed the verdict as a judicial intervention.

Amidst this impasse, the Army chief stepped in to resolve the situation by organizing talks between the different conflicting factions. The talk ended in another deadlock, prompting the army chief, who later became leader of the NCPO, to announce a seizure of power. It merits observation that the coup was announced a few days after the enforcement of martial law to curb sporadic violence in the capital city.

To many, the bloodless coup in May was welcomed and seen as inevitable to end the stalemate between the conflicting factions, as well as the rising violence that accompanied the political conflict in many rally venues. Notably, the political conflict in Thailand in the last decade was often dubbed "color-coded politics" to describe the ideological clash between the yellow-shirts[4] and the red-shirts,[5] who represent two opposing poles in the contemporary political divide.

---

[4] The "yellow-shirts" is another name for the People's Alliance for Democracy (PAD), a mass movement preceding the September 2006 coup that ousted Thaksin from the premiership. The PAD spent much of 2008 protesting against two successive Thaksin-nominated governments that arose from the December 2007 election. The PAD's 190-day protest in 2008 was marked by the seizure of the Government House and the Suvarnabhumi International Airport in Bangkok. In 2009, leaders of the PAD entered electoral politics by establishing the New Politics Party. One of the PAD's leaders, Sonthi Limthongkul, is a media mogul who has been instrumental in using his media corporation particularly a satellite television station called ASTV as a main tool to galvanize mass movements in support of the PAD. After the 2017 coup in May, ASTV was banned from airing signals.

[5] The "red shirts" is the informal name for the United Front of Democracy against Dictatorship (UDD), a major political organization in the post-coup period. Members of the UDD are known for wearing red clothes during anti-government protests. Established in 2006 as Democratic Alliance against Dictatorship (DAAD), the main objective of the red shirts then was to fight against its arch rival -- the PAD -- and to support the ousted former Prime Minister Thaksin Shinawatra. Supporters of the UDD are not only rural grassroots people who benefited from Thaksin's populist welfare policy, but also include the urban middle class who admire Thaksin's business-oriented administrative policy and action, and those who disapproved of the status quo that formed the core of the yellow-shirts.

Media – big and small, online and offline – have been used to propagate and widen this political polarization, sometimes resorting to hate speech.

After the coup, a series of coup notifications were released to the public, including about a dozen that put tight controls on communication, including online social media. Internet service operators were summoned to meet with the junta, who requested cooperation in reporting and dissemination of junta information, and barred these operators from instigating unrest and criticism of the junta and their work. There was also a brief period of inaccessibility to Facebook, which was suspected to be coup-related, although the NCPO denied any involvement

B. Social Development Related to Online Intermediaries

In terms of Internet statistics, there are 23.8 million Internet users in Thailand, representing 35% of the population.[6] Mobile telephone users are numbered at around 120 million, based on the number of SIM cards distributed.[7] Around 40% of mobile users access the Internet via their smart phones, which most use to view online social media like Facebook, Instagram, and Twitter.[8] Bangkok has been ranked as the capital city with the highest number of Facebook users in the world.[9] Meanwhile, "LINE," a mobile chat app that was developed by Japan-based LINE Corporation, is also extremely popular in Thailand. The country has the most LINE users of any country outside of Japan, with 61.1% of social media users – about 18 million – said to be using the application.[10]

Online intermediaries play a critical role in social development in Thailand, particularly in the protracted political conflict that the country has been embroiled in since 2005. In the latest political crisis that has developed since October 2013, social media became a key online channel for people to keep abreast of the current political climate, as well as to mobilize resources in support – as well as in defiance – of the protest movements.

During the seven month-long protest against the popular but polarizing government of Yingluck Shinawatra, online media usage across services like Facebook, Twitter, Instagram, LINE, and Pantip.com (a popular online discussion form) in Thailand was very dynamic. In the first month after the protest began, for instance, Twitter was found to be the most used social media channel for protesting the controversial draft amnesty bill – the catalyst of the lengthy protest – with over 800,000 messages sent in one peak day in November 2013.

C. Regime of Internet Content Regulation

As for Internet regulation in Thailand, a number of entities are involved. The Ministry of Information and Communication Technology (MICT), established in 2002, is the central organization that implements the Computer-related Offences Act B.E. 2550 (2007), better known as the computer crime law, along with the Technological Crime Suppression Division (TCSD) of

---

[6] 2014 Asia-Pacific digital overview from http://wearesocial.sg/

[7] Survey of Thailand's communications market 2012-2013, Center for Telecommunications Economy Data and Research, National Broadcasting and Telecommunications Commission.

[8] Info graphics of Thailand mobile users, 2013. See http://www.veedvil.com/news/thailand-mobile-in-review-q3-2013/

[9] http://www.socialbakers.com/facebook-statistics/thailand

[10] http://www.veedvil.com/news/thailand-mobile-in-review-q3-2013/

the Office of National Police. The National Broadcasting and Telecommunications Commission (NBTC) regulates licenses for Internet services and International Internet Gateways. Therefore, all Internet service providers report to the NBTC under licensing obligations, while also being subject to the MICT's Internet content filtering scheme.

Apart from prosecuting offences under the computer crime law, the MICT has also conducted constant surveillance and censorship of online content through specially recruited cyber-scouts and URL blocking via ISPs. Since the arrival of the computer crime law in 2007, court orders to block Internet content have increased from two URLs in 2007 to over 74,000 in 2012.[11] Examples of content targeted for filtering include lèse majesté or defamation of the royal family, drug trafficking, gambling, and prostitution, which are not necessarily offences as stipulated in Section 14 of the computer crime law that addresses content offences.[12]

According to a report published by iLaw, an online rights-based NGO, most of the offences prosecuted under the computer crime law are content-related.[13] Since the law came into effect in 2007, both the number of cases prosecuted and the number of websites that have had access blocked have increased, which coincided with the looming political conflict and polarization that has characterized Thai society in recent years. Cases involving lèse majesté, which is a serious crime in Thailand, were also on the rise in both online and offline communications during this period.

D. Internet Control in Pre- and Post-2014 Coup

During the highly volatile period under the Yingluck administration, the TCSD was pro-active in policing websites and online social media. In one instance in August 2013, the TCSD reportedly attempted to probe the conversations and comments posted on the highly popular social-media application, 'Line', to see if they violated the law or threatened national security. This incident was preceded by the summoning of four suspects for allegedly breaching Section 14 of the computer crime law and Section 116 of the Criminal Code by posting messages via social media, saying they anticipated a coup and urged people to stock up on food and water. These statements, according to the TCSD chief, could put people in a state of panic, and those who "liked" or "shared" the messages could be considered violators of the law as well. An open letter of opposition from four professional media organizations and an online rights-based group met the TCSD's action. Meanwhile, the National Human Rights Commission also issued a statement

---

[11] Suksri, Sawatree, et al., *Situational Report on Control and Censorship of Online Media through the Use of Laws and the Imposition of Thai State Policies* (Bangkok: iLaw and Heinrich Böll Foundation Southeast Asia, 2010).

[12] Section 14 of the law provides for imprisonment for up to five years and/or a fine of up to 100,000 baht (approximately US $3,000) for these content-related offences. These offences are referred to as "import into a computer system," of the following: 1) false data in a manner likely to cause damage to a third party or the public; 2) false data in a manner likely to damage national security or to cause public panic; 3) data constituting an offence against national security under the Criminal Code; and 4) pornographic data that is publicly accessible. The dissemination or forwarding of computer data in the nature under 1), 2), 3), and 4) are also offences and subject to the same criminality.

[13] Suksri, Sawatree, et al., *Situational Report on Control and Censorship of Online Media, p. 5.*

warning police to exercise their authority carefully and not violate people's fundamental rights and freedoms.[14]

Since the coup on May 22nd, 2014 that toppled the Yingluck government and ended the months-long political crisis, the surprisingly popular junta known as the National Council for Peace and Order (NCPO) has taken steps to restrict the spread of anti-coup sentiment. First, an order known as the NCPO Announcement was released on the day of the coup that called on ISPs to monitor and deter the publication of online information that might incite unrest in the country.

Then, another order was launched that summoned all 105 local ISPs to meet with the junta-appointed Cyber Security Operation Center (CSOC), in addition to representatives from major online intermediary services in the country, including Google, Facebook, Twitter, YouTube, Instagram, and LINE, to discuss "cooperation" on the issue. That meeting, however, did not materialize as the invited companies failed to show up. Another scheduled trip to Singapore of the CSOC staff to meet with Facebook, Google, and LINE was also called off after it was deemed unnecessary.

Notably, Facebook was the first social media platform to experience blocking on May 28th, when it was inaccessible for about one hour. The outage was initially blamed on technical issues at the country's gateway, but an MICT spokesperson later said that the action was intended to stop the spread of anti-coup messages. A Norwegian telecom firm, Telenor, which owns majority shares in the country's second largest GSM mobile phone provider, later confirmed this.

III. Laws, Past Prosecution, and Recommendations for Change

This section reviews relevant legislations and measures that contain provision(s) related to online intermediary liability; a case study on intermediary liability prosecution; and recommendations by a key civil society stakeholder on ways to alleviate the impacts from Internet Thailand's intermediary liability scheme.

A. Computer-Related Offences Act B.E. 2550 (2007)

This law (better known as the computer crime law), the first of its kind in Thailand, was enacted in 2007 by the National Legislative Assembly (NLA), an interim legislature that was installed by the military junta in the aftermath of the 2006 military coup that toppled the civilian government of Thaksin Shinawatra. Although there had been many versions of the draft law before, its passage immediately after the coup was seen by many as a direct effort to curb online dissent that formed largely in cyberspace since the conventional media sector – print and broadcasting – was tightly controlled by the coup-leaders.

Apart from sections that address crimes to computer systems, such as hacking, viruses, and electronic sabotage, the law also has specific provisions that address content offences. Section 14 of the law provides for imprisonment for up to five years and/or a fine of up to 100,000 baht

[14] Puengnetr, Pakorn, Asina Pornwasin, Chanikarn Phumhiran The Nation August 13, and 2013 1:00 Am. "Police Seek to Check Line Posts." *The Nation*. http://www.nationmultimedia.com/politics/Police-seek-to-check-Line-posts-30212462.html.

(approximately US $3,000) for these content-related offences. These offences are referred to as "import into a computer system," of the following: 1) false data in a manner likely to cause damage to a third party or the public; 2) false data in a manner likely to damage national security or to cause public panic; 3) data constituting an offence against national security under the Criminal Code; and 4) pornographic data that is publicly accessible. The dissemination or forwarding of computer data under items 1-4 are also offences and subject to the same criminality.[15]

Section 15 of the law is the centerpiece of the intermediary liability provision. It states that, "A service provider who intentionally supports or gives consent to the commission of the offences under section 14 to a computer system under his control shall be liable to the same criminality as the offender under section 14."[16]

While the two sections in the law deal exclusively with content offences, they do not make any distinction between the different types of intermediaries – those that deal directly with content – online service providers – and those that are merely conduits for the content – network and access providers. In other words, all online intermediaries are subject to the same liability for offences they do not commit, but take place within the network or communication space provided by them.

In a related vein, critics have also attacked the lack of clarity in the definition and implementation of the law.[17] Usually a public law would entail the subsequent issuance of a ministerial order that would provide more detail about how the law may be enforced. For instance, a ministerial order on the computer crime law might spell out what constitutes false information, or what the categories of information constitute causing harm to national security, or the reasonable period of time that an intermediary is provided to remove illegal content after having been given a notice before being considered negligent or giving consent to the offence. Unfortunately, such a ministerial order does not exist in this situation.

Since the law came into effect, a few tangible impacts can be observed: the legalization of Internet blocking, indirect regulation via intermediary providers, and self-censorship of online content providers. Based on primary research findings,[18] online intermediaries of all types have set up new measures to regulate content and, in the process, are passing regulatory constraints onto users. These measures include the following:

- Keeping a log file of Internet traffic, including users' IP addresses, for 90 days;
- Identification and certification clearance requirements for users at institutional servers and for subscribers to online discussion forums;

---

[15] Translation of the Computer-Related Offenses Act, Vol. 124, Section 27 KOR, Royal Gazette. 18 June 2007, p. 7. Available at http://www.itac.co.th/index.php?option=com_content & view =article & id=90.

[16] Ibid.

[17] Sinfah Tunsarawuth and Toby Mendel, *Analysis of the Computer Crime Act of Thailand* , http://www.law-democracy.org/wp-content/uploads/2010/07/10.05.Thai_.Computer-Act-Analysis.pdf .

[18] See more in Pirongrong Ramasoota. Internet Politics in Thailand after the 2006 Coup: Regulation by Code and a Contested Ideological Terrain. In Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds.), Access Contested: Security, Identity, and Resistance in Asian Cyberspace, pp. 83-114. Cambridge: MIT Press, 2012.

- Installing filtering software at organizational servers to enable content filtering;
- Setting up a 24-hour monitoring system for online discussion forums; and
- Incorporation of provisions of the law into codes of ethics/practice and terms of services.

Although the law has only been enforced for a few years, it has come under heavy criticism largely by Internet providers and online activists, both locally and internationally. Local rights-based NGOs have been mobilizing for an amendment to the law but, with the chronic instability of Thai politics in recent years, this amendment has been pushed back. And in the current coup-controlled environment in which free expression is the exception rather than the rule, it is unlikely the amended version of the law, if it proceeds, will reflect a more liberal tone than the existing law.

B. National Council for Peace and Order (NCPO)'s Announcements

Historically, revolutionary decrees and coup announcements in Thailand have been seen as equivalent to laws and have had lasting effects. Because of the need for social control during such periods, many of these legal statutes are designed to specifically curb the right to free speech, particularly that of the media. Such a notion of control might have been understandable in the context of conventional media like newspapers or broadcasting, where centralized outlets of dissemination may be controlled during such problematic times. However, with the highly distributed nature of network technology like the Internet, particularly online social media that relies almost entirely on users to generate content, it is almost unthinkable to impose control upon these communication platforms.

Nevertheless, such was the case with two of the NCPO's Announcements that emerged on the day of the coup itself, May 22nd, 2014. In Announcement No. 17/2014 entitled "The Dissemination of information via the Internet," all Internet service providers were instructed to comply with the following orders:

- Monitor, investigate, and halt the dissemination of any information that may distort, incite, or instigate unrest in the kingdom or that might affect national security or public morality;
- Appear at the 2nd floor meeting room of the Office of the National Broadcasting and Telecommunications Commission (NBTC) on May 23rd 2014 at 10.30 hours.[19]

As a result of the second provision in the above announcement, a total of 108 Internet service providers were summoned to meet with NCPO staff at the Office of the National Broadcasting and Telecommunications Commission (NBTC) on the specified date.

At the meeting, attending representatives of the ISPs were told to block public access to the Internet addresses of web pages or content deemed to be violating the coup orders, and to IPTV or live TV broadcasts relayed via Internet that were similarly in violation.

[19] National Council for Peace and Order Announcement No. 17/2014. In Thai (Translated by author)

Based on news reports of the meeting, a working committee of the NCPO would inform the ISPs to block access to certain Internet addresses on a case by case basis, as the coup maker did not plan to block general online communications but rather wanted to block access only to content that violated the coup orders.[20]

In another announcement, No. 18/2014 on the topic of "Dissemination of information to the public," all operators of mass media – print, broadcasting (terrestrial, cable, and satellite), electronic, and online social media – were asked to refrain from presenting information in the following manner:

- False information that may be defamatory, and foster hatred directed towards the royal family;
- Information that may be harmful to national security, and defamatory to another person;
- Criticism of the operations of the National Council for Peace and Order (NCPO), its staff, and related persons;
- Voice, picture, video that may be official secrets;
- Information that may cause confusion, incitement, or instigation of unrest or division in society
- Invitation to participate in or assembly that may lead to protest against the NCPO and its staff;
- Threats to harm a person that may lead to public panic and fear.[21]

According to this Announcement, it is also mandatory for all media to disseminate information issued by the NCPO.

On July 19th, 2014, the NCPO issued another announcement which in effect merged the above two announcements into one, but with an added clause threatening sanctions. This controversial NCPO Announcement No. 97/2017 has the perceived "chilling effect" paragraph at the end, which says that, "failure to comply with orders in the announcement will result in an immediate ban of the media in question and, subsequently, legal action."[22] This order was widely frowned upon by members of the media and general media users, who viewed the announcement not only as curbing free expression, but also as limiting individuals' right to knowledge. After a few days of negative feedback, the NCPO decided to issue another announcement in replacement – NCPO Announcement No.103/2017 – that did away with the media ban and legal action but replaced it with a provision that forwarded problematic cases to related professional media organizations for immediate action. Additionally, the problematic content must be false and exhibit intent to discredit the NCPO to warrant action.

C. Past Prosecution and Regulatory Measures on Online Intermediaries

Thus far only one case has been prosecuted relating to intermediary liability in Thailand. This was the case of the moderator of a progressive online discussion forum who was prosecuted for

[20] http://www.nationmultimedia.com/politics/ISPs-told-to-block-pages-content-seen-as-violating-30234447.html
[21] National Council for Peace and Order Announcement No. 18/2014. In Thai (Translated by author)
[22] National Council for Peace and Order Announcement No. 97/2014. In Thai (Translated by author)

intermediary liability under lèse majesté – defaming members of the royal family. A summary of her arrest and trial is provided below.

1. Chiranuch Premchaiporn and Prachatai Case

Chiranuch Premchaiporn was moderator of the online discussion forum attached to an online newspaper called *Prachatai.* In September 2010, Chiranuch was arrested and later charged with committing an offence under Section 15 of the computer crime law and with lèse majesté as a result of 10 comments posted in the forum's board that were deemed royally defamatory. According to reports, the police had notified *Prachatai* staff to take down the illegal content and most of the content was deleted except for a few pieces that remained for several days.

As Chiranuch recounted in some news reports, there were too many postings to keep pace with as the forum became very dynamic in the highly volatile context following the crackdown on red-shirt protesters in May 2010. Many red-shirt supporters were frustrated and vented their anger on the *Prachatai* web forum, which was known to be an alternative and rather left-wing space. Participants on this board were also known to be sympathetic towards the red-shirt movements.

Chiranuch went to trial in 2011, facing criminal charges since lèse majesté is an offence against national security under Section 112 of the Criminal Code. One year after the beginning of the trail, which drew significant international attention but little local coverage, in 2012 the Criminal Court found Chiranuch to be guilty and handed down a one-year prison sentence, then reduced it to an 8-month suspended prison term and a 20,000 baht (about US$680) fine.

The verdict stated that since the provision in the computer crime law did not specifically give a clear timeframe for taking down problematic content, it would be unfair to expect the web operator to preemptively delete the content. Yet, the court did not uphold the claim by the defendant (Chiranuch) that she had no knowledge of the defaming content being imported into the system because the police had notified Prachatai, yet one of the comments was left for more than 10 days before being deleted. As a web moderator, the defendant (Chiranuch) was expected to perform her duty by taking into account the intermediary liability provision. According to the verdict, illegal content that is left up for too long could lead to damages to related persons and – if disseminated irresponsibly – could cause adverse impacts to national security.

The court pointed out that there was one posting that was left on the forum's board for a total of 20 days, which is an extensive period. The web moderator's failure to act swiftly enough was construed as giving consent for the illegal content to remain, despite being notified. For this reason, the court ruled that the defendant was guilty as charged.

Compared to previous lèse majesté cases, this court's ruling reflected leniency for Chiranuch, who could have faced up to 20 years in prison. For international observers from rights-based groups, the case was seen as a test of free expression involving online intermediaries in Thailand. After the eight-month suspended sentence ended, Chiranuch lodged an appeal against the verdict in 2013 and is now awaiting the result. Meanwhile, the *Prachatai* web board has become defunct, as the organization could not bear the costs of around-the-clock monitoring with its limited funding and staff.

D. Recommendations From Civil Society on Alleviating Impacts from Intermediary Liability

The Thai Netizen Network (TNN), a local NGO that advocates for Internet freedom and online communication rights, gave the following recommendations regarding online intermediary liability enforcement in Thailand:

- Internet service providers and caretakers must be classified into two groups – content-related and not content-related;
- Those providers and caretakers that are not content-related must be exempt from liability;
- A proper regulatory framework must place the liability of providers and caretakers of content-related entities in accordance with their proximity to the content;
- Regulators and law enforcement agencies must minimize the scope of impact when issuing notifications for blocking content. Those with the most proximity to the problematic content should be notified first, followed by those with less proximity. This is so that those that are closest to the content can most effectively manage the situation, while minimizing the impacts on others that are not directly related;
- Blocking access to content must be a temporary measure to alleviate the damage. Block orders can only be enforced in the presence of a court order, as a result of a charge or a lawsuit in trial. The block period must also be defined explicitly (although expandable within a time limit);
- In blocking access to content, service providers must clearly show the number of the court order on the website for public verification; and
- Content blocking must cease in cases where there is no arraignment or trial, or the lawsuit ends with a not guilty verdict. All details of the lawsuit and trial must also be publicized.[23]

IV. Research on Local Intermediaries and Their Content Practices

In order to explore first-hand how different intermediaries view the intermediary liability law and the ways that they are coping with the scheme, questionnaire-based interviews were carried out between April and June 2014 with 20 online intermediaries in Thailand. Of these, five were network providers, four were Internet service providers (ISPs) or access providers, and 12 were content providers.[24] The last group was comprised of hosting services, online news websites, online discussion forums, social networking services, electronic commerce websites, specialty content providers, and web portals. Names of all interviewed organizations and the interviewees cannot be provided as they agreed to be participants provided that their personal information and information about their organizations be kept anonymous. For the sake of academics, however, it

[23] https://thainetizen.org/docs/netizen-report-2013/

[24] Network providers here refer to those operators of Internet Gateway (IIGs) as well as National Information Exchange (NIX) which rent out their networks to ISPs or general users and the scale of their service can affect the public interest. Access providers are ISPs that do not have their own infrastructure but provide access to the Internet to organizations or entities or individual users. Content providers are those that provide a variable of content services to online users and do not need to own a network to provide the services.

may be useful to note that all the interviewed intermediaries were local operators. Effort was made to tap US-based providers of major online social networking services, but this was unsuccessful.

The interviews were structured around many salient points as experienced by network, service, and online intermediaries on content regulation, burdens incurred from intermediary liability provisions, content-filtering practices, perceived impacts from the computer crime law, and the assessment of impacts from the current coup-controlled regime.

The following is a summary of these important points and the opinions of interviewees that represent the Internet/online provider sector.

- Burdens imposed on intermediaries;
- Content filtering practices;
- Types of content filtered;
- Transparency and accountability in content regulation;
- Impacts of intermediary liability provision; and
- Impacts of Internet control under coup.

A. Burdens Imposed on Intermediaries

The interviewed intermediaries were asked to rate the perceived level of burden imposed on them as a result of intermediary liability provisions in two aspects – allocation of resources and legal responsibility.

Most of those interviewed feel that the current burden being imposed on them regarding intermediary liability in ordinary periods is acceptable and only a few think that they are being overburdened. See Figure 1 for details.

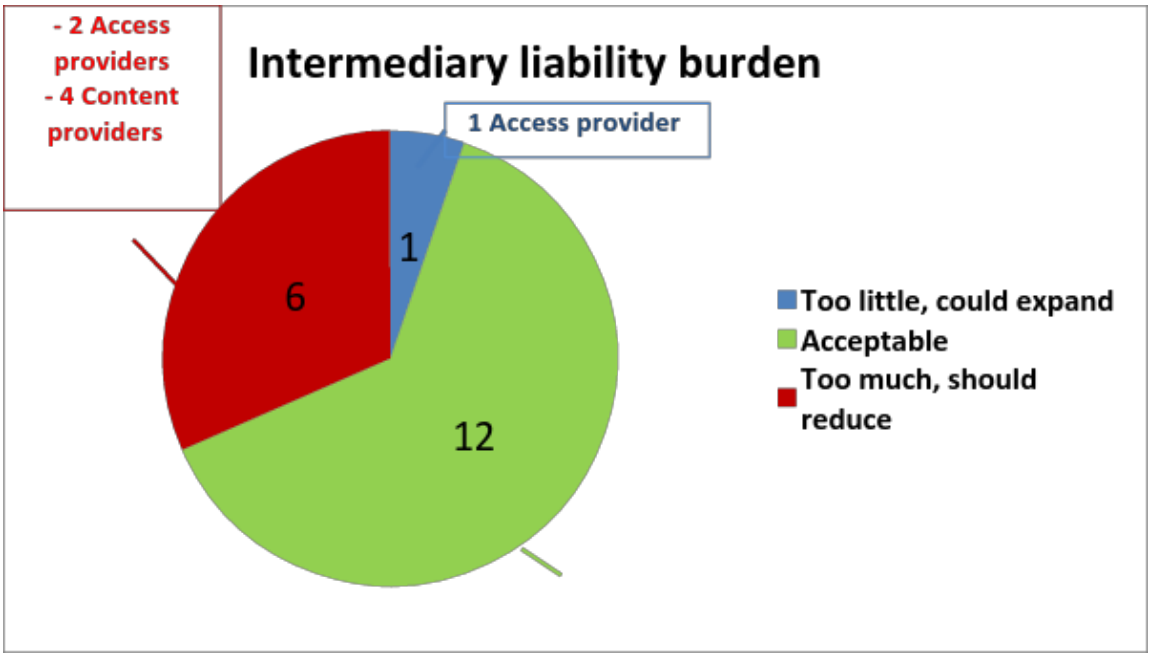


Figure 1: *Level of intermediary liability burden as perceived by online intermediaries*

However, a couple of ISPs made a critical note of the high and quite unproductive costs of having to keep traffic logs for 90 days, as well as having to install content filtering systems. In terms of human resources to patrol for content offences, at least five providers across several categories reported that specialized personnel were needed for this task. According to a couple of network and access providers, they needed to recruit new engineering staff and to develop new filtering tools to guard against problematic content. Meanwhile, operators of two online newspapers reported that they had to assign senior reporters/editors with sufficient legal knowledge to help supervise content.

As for the legal responsibility compelled by the intermediary liability provision, all access providers interviewed feel that the law is quite unreasonable to impose such liability conditions. Considering that intermediaries are not the offenders and thus could not have the intent to the commit crime, to hold them liable is unfair, according to one access provider. Most of the interviewed content providers also hold this view. While operators are expected to be vigilant to guard against problematic content, it is quite impossible in practice for this monitoring to be completely foolproof. As with any reasonable deliberation in a criminal case, they strongly feel that "the intent to commit a crime" should be a necessary basis for judicial judgment.

In addition, the interviewed providers feel that the penalties – imprisonment and fines – are not proportionate to the "offence," which is oftentimes an unintentional error or oversight. Among the content providers, which are the category of intermediaries most apprehensive of the law, those that appear most antagonistic are those that deal with relatively sensitive content like investigative reporting and those ISPs or hosting services with online forums that thrive upon content generated by users. As reported by these interviewed content providers, most of the problematic intermediary cases they have faced are state-intermediary-user cases, rather than user-user conflicts. The latter is manifested more viably in online forums, and stems mostly from copyright infringements and defamatory remarks. However, most of these cases were sorted out or settled with the intervention of the forum moderator and very few progressed to litigation, though usually not on intermediary liability charges.

B. Content Filtering Practices

When asked about content filtering practices, it is interesting to find that network and access providers are the group that reports the highest frequency of content blocking in accordance with court orders. All the content providers interviewed said they have never blocked content from court orders because they have never been served with one. This is understandable given the structure of Internet regulation in Thailand, in which only network providers and access providers are licensees under the National Broadcasting and Telecommunications Commission's system and are thus identifiable to the authority.[25] See Figure 2 for details.

[25] Under the NBTC's Internet providers licensing system, there are two types of licenses. Type 1 license refers to license for operators who do not have their own network infrastructure and must strictly concentrate on concentrate on providing only Internet access and related services to users who are individuals, organizations, or entities, both public and private. Type 2 license is subdivided into three classes: 1) license for operators of international Internet gateway (IIGs) and national information interchange (NIX) without their own network infrastructure that render services to specific groups of customers in such a way that may not affect the larger public interest; 2) license for operators of international Internet gateway (IIGs) and national information interchange (NIX) with their own network infrastructure that service specific groups of customers in such a way that may not affect the larger public

In any case, court orders are usually administered through the Ministry of ICT (MICT), which is in charge of content regulation in Thailand. But since MICT does not control the licensing system, they cooperate closely with the NBTC to whom ISPs directly report.

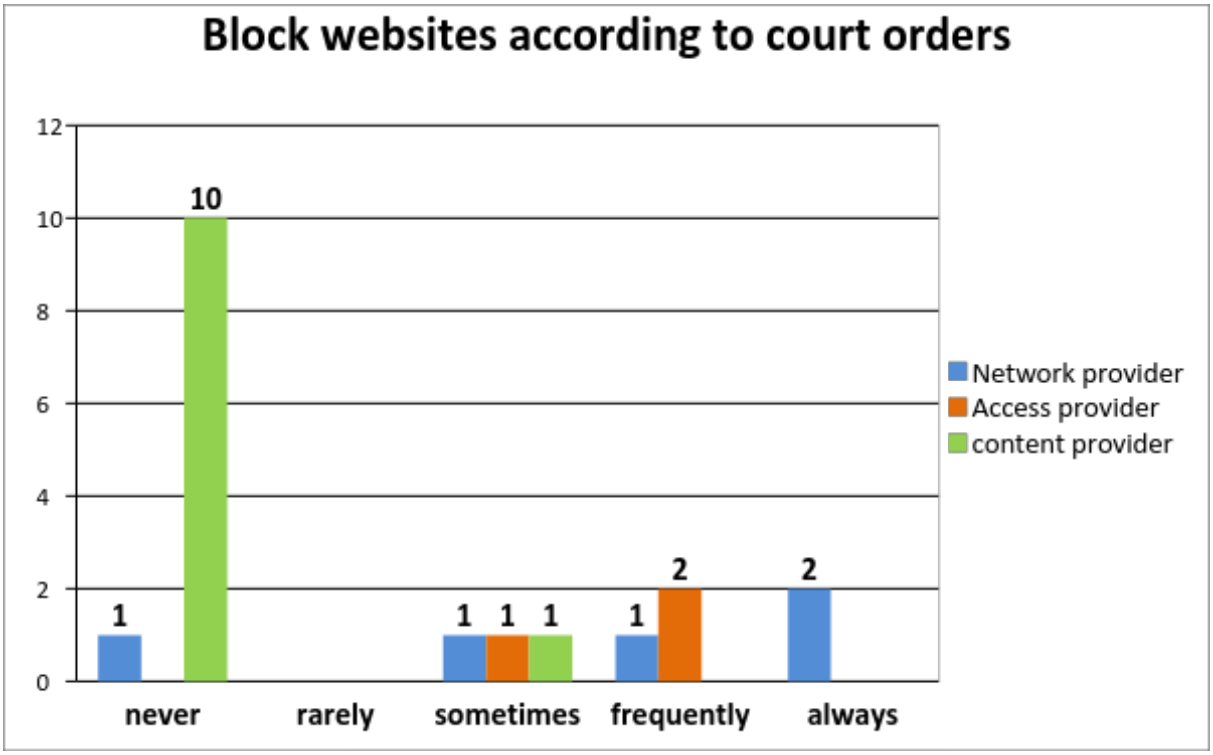


***Figure 2**: Frequency in blocking websites according to court orders*

Another interesting finding is that the larger the scale of the provider, the higher the rate of website blocking in accordance with court orders. From the interview in which the operators were asked to rate the frequency of the blocking based on court orders, the country's two largest network providers both give the highest score. This correlates with a revelation about the likelihood of being served with a notice and takedown request from the authorities. The larger the operator (in terms of customer base and popularity), the more likely they are to have received notification from the authorities. Many smaller and less known websites and operators reported never having been served with a notice and take down request.

On the other hand, when asked about their content blocking and take down practices that stem from notification by officials or general users of content that is not illegal (but potentially harmful) in the absence of a court order, most of the providers in all categories (though principally in the network and access provider categories) reported that they never comply with such notifications. See Figure 3 for details.

interest; 3) license for large Internet Service Providers, that may perform as IIGs or NIXs, but have a large scale of customers and their services may affect the larger public interest or free and fair competition in the market.

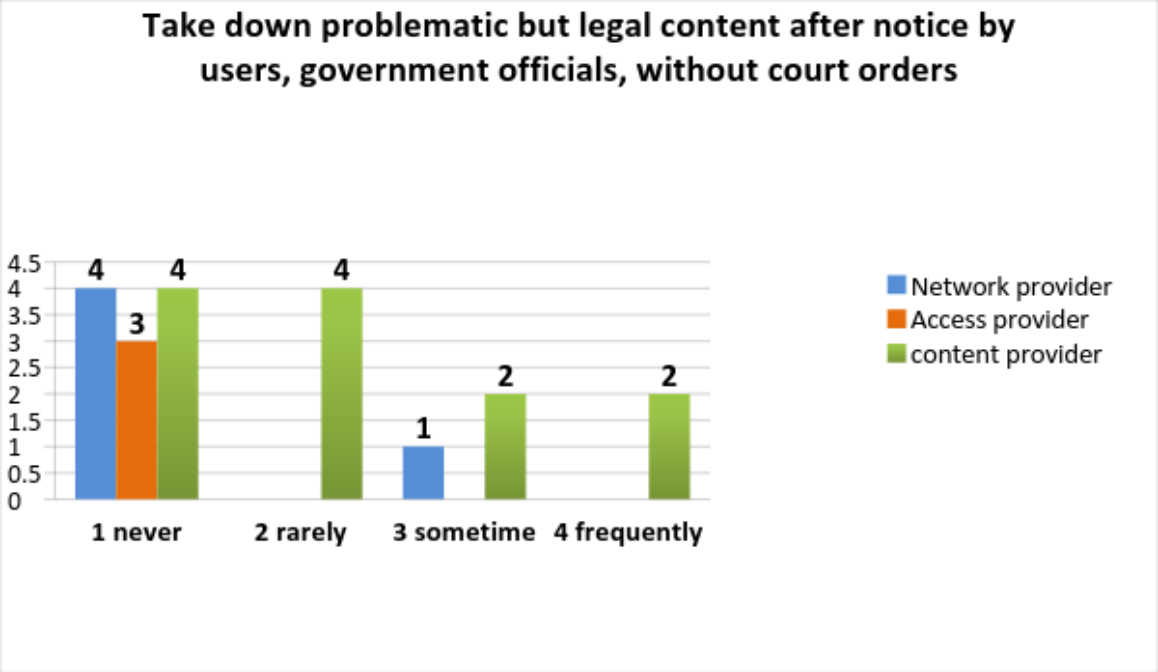


***Figure 3**: Taking down problematic but not illegal content according to notification by users or officials in charge, without a court order*

However, some content providers that operate services with an extensive amount of user interaction, like online discussion forums, operators of the Facebook page of an online newspaper, or news blogs with readers' comments, said that they occasionally remove content that is reported by their users who constitute a community of sorts. In this community, a certain form of self-regulation based on ethical guidelines and terms of use published by the website has taken shape, and played a role in guarding against unwanted content.

Apart from blocking as a result of court orders and taking down content without court orders, the intermediaries were also questioned about whether they administer their own content filtering systems voluntarily. See Figure 4 for details.

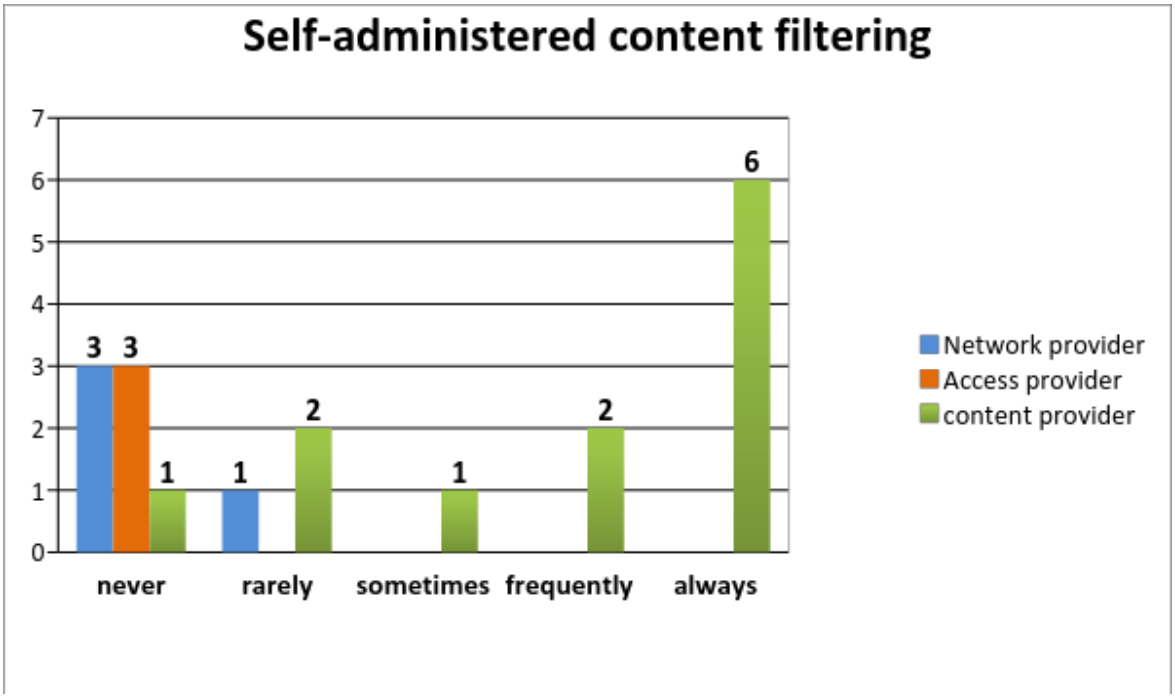


***Figure 4**: Frequency in self-administering of content filtering by intermediaries*

Eight out of nineteen interviewees reported that they frequently to always administer their own content filtering. This includes three online news website operators, two online discussion forums, one specialty website, and one electronic commerce website. Their most common reason for this content filtering was to minimize the risk of lawsuits, not only stemming from content crimes but also copyright infringement and defamation.

As for network and access providers, all except one do not administer their own filtering or use their own judgment in blocking out content. This is because they feel that it is beyond their role and authority to make such decisions. The access provider that was the exception is a state enterprise, which installed a filtering system on their network many years ago. Yet, a representative from this organization reported that content is rarely blocked as a result of their independent filtering system.

C. Types of Content Filtered

The types of content – illegal or otherwise – which different types of intermediaries report to have filtered varies somewhat in accordance with the priorities of each operator. However, lèse majesté, which is a severe offence and deeply rooted in Thai society, topped the charts of all three types of intermediaries for takedowns, followed by national security. Overall, the block list of network and access providers is indicative of the content offences outlined in Section 14 of the computer crime law. See Figure 5 for details.

Network providers	Access providers	Content providers
1) lèse majesté 2) national security	1)lèse majesté 2) national security	1) lèse majesté 2) doctored image that

3) false information that could lead to public panic 4) pornography 5) gambling	3) false information that could lead to public panic 4) pornography 5) gambling	may be defamatory 3) copyright 4) gambling 5) hate speech

Figure 5*: List of top content categories blocked or removed by different types of online intermediaries*

The similarities shared by network and access providers may be attributed to the fact that both function mainly as conduits for information and are governed under the licensing system, and are therefore in closer proximity to the government's structural regulation of the Internet. Their forbidden content list is in effect derived from the block lists issued by MICT, with or without court orders.

Meanwhile, the variation reported in the content providers' list, with the exception of lèse majesté, can be accounted for by the specific content orientation of each website and the fact that they operate more closely to the content than network and access providers, while being more distant from the official structure of Internet regulation. In some cases, providers also take down content that is not illegal but may be harmful, such as hate speech or content related to drugs. An operator of a popular online discussion forum, for instance, gave high priority to hate speech, which has been a growing online phenomenon in Thailand despite the fact that this is not a crime under Thai law.

Another interesting observation that emerged from this part of the survey is that other than following court orders, most network and access providers usually consult with the MICT in any dubious content take down decisions. Most content providers make such decisions independently, though the few that are big enough to host a legal unit will consult with their lawyers before making such decisions.

D. Transparency and Accountability of Content Regulation Process

Although most interviewed intermediaries assure that they operate their content handling with transparency, only about half of those surveyed publicize or make available their content regulation guidelines or filtering process to their users. Those that do have the information available claimed to have content guidelines incorporated into their terms of use, while only a couple provide the users with information about content filtering process.

Interestingly, neither of the two network providers interviewed – a state enterprise and a private corporation – have such information available for their customers. Both justified this absence by the fact that all filtering protocols and practices are done as part of the working procedure of the Ministry of ICT. The intermediaries' role is to just comply and render the sought co-operation. The same is true of all the interviewed access providers who claimed that all necessary information about blocking/filtering was publicly provided in the block pages of the MICT, and now the NCPO's block page.

Most of the intermediaries studied have many channels (e.g. telephone, mailing address, online social media, and website) for users to file a complaint about their services, including a notice for

content take down. However, very few provide a channel for complaints or petitions against blocked or removed content. For those network providers that do not provide such channels, they claim that the decision to block content is final as it is a legal action in accordance with court orders. If any complaint on such procedures is to be made, it must be directed to the authority that ordered the blocking, whether it is the court or the MICT-appointed officials.

Similarly, the usual content filtering procedures carried out by these intermediaries do not include notification to users or websites in cases that their content may be blocked or removed. All network and access providers state that they do not have this policy and practice in place for the same reason as above. They also feel that since they have a large base of users, it would not be feasible to circulate such notifications and that this should be the duty of content provider, not the intermediary, to do this.

Meanwhile, most content providers that do perform their own filtering also do not routinely give notification before taking down content. This is because they feel that the reason for their decision is already indicated in the terms of use and content guidelines. Of all the interviewed content providers, four claimed to occasionally notify their clients or users about content removal in cases where the offence is not legally conclusive. But in cases where the content falls clearly under the law, they will automatically remove without notifying.

Notably, of all the studied intermediaries, only the operator of a famous online discussion forum website has a standard practice of notifying users before and after content removal. Prior notice is sent directly to the individual user, with an explanation as to why his or her posting is being removed. A notice after the content takedown is also sent to each individual user after a certain number of wrongdoings are committed. This is to remind the problematic user that his or her account may be revoked as a result of these wrongdoings.

In addition, most intermediaries in the study also claimed they have in place preventive measures against business bullying or discrediting in cases of notice for content takedown from users. Some intermediaries require that the person(s) who lodged the complaint to press charges with the police to help verify the identification and credentials of the complaint filer. Others use an in-house committee to help scrutinize the complaints more thoroughly. Some content providers also have their staff investigate into past use records of the complaint filer to check their reliability. But there are quite a significant number of intermediaries, mostly network and access types, that do not have such procedures in place as they do not respond to users' takedown notice and act only under the instruction of the MICT or a related authority.

When questioned about the integrity of their content regulation system, all intermediaries assured that they maintain good practice and good governance. While the studied network and access providers tend to emphasize data security, technological safeguards, and quality assurance systems, the content providers are more inclined to show that they adhere to professional ethics, particularly those in the online news sector. As for those non-journalistic content providers, they claim to have a transparent system that is open to scrutiny, both internally and externally. However, a couple of the intermediaries in the study feel that ensuring integrity of content regulation processes should be the duty of the regulator or the National Broadcasting and Telecommunications Commission (NBTC), while another intermediaries see compliance with court orders as already sufficient to show integrity in this regard.

E. Impacts of Intermediary Liability Provisions

All intermediaries in the study admitted that the intermediary liability provision has had an impact on their work and the way they conduct their business. Apart from the increased burden mentioned earlier, many intermediaries also expressed frustration in complying with the law, which they feel is incongruous with the open and participatory nature of the Internet. According to one access provider, the main discrepancy in the law lies in holding intermediaries liable for content that is imported into the system under their care, but not giving access providers the right to filter the content independently. The authority to take down content is centralized under the court system.

Meanwhile, another access provider objected to the idea of access providers having to monitor and filter content, as this would entail tremendous and unnecessary costs. If anyone in the supply chain of Internet content should be responsible, it should be the content providers who are closest to the content.

Since the law came into effect seven years ago, at least three of the surveyed content providers said they had held regular training for their staff to educate them about provisions in the law, while a blog hosting service provider has had to assign a blog editor to supervise content within their hosting space. For online newspapers, 24-hour content monitoring became mandatory, particularly for the users' comment section. Those who could not cope with the rising costs and burden would have to discontinue interactive functions like online forums, while others who did not have interactive features decided to maintain their online services' one-way communication structure to minimize risks.

Over all, most of the intermediaries studied object to having the intermediary liability provision in the computer crime law. This includes almost all the network and access providers, with the exception of two that feel holding intermediaries liable is fair and will lead to more responsible use of the widely diffused and all-encompassing Internet. Those who object to the law see intermediaries as messengers or conduits of information and, thus, believe they should naturally be exempted from legal responsibility. One of the network providers argued in support of an international principle imbued in the European Cybercrime Convention that protects intermediaries, and urged that this be adopted in the new and amended version of the computer crime law.

Within the content providers' segment, the view is split into two poles. There are those that disagree with holding intermediaries liable under any circumstances, and those that see intermediary liability as necessary, particularly for Internet applications and space that rely on user-generated content, like online public forum and comments sections. For the latter group, the malleability of the Internet, which makes it highly flexible to copy, share, and disseminate information to the widest audience, is a sufficient justification for imposing liability. For this group, a website operator is comparable to a landlord. The duty of the landlord is to make sure that all tenants take good care of their own space and do not break the law while in residence.

F. Recommendations for Changes to Intermediary Liability Provisions

Most of the intermediaries propose that if the law is to be amended, it should adopt an approach that protects intermediaries. These are some such suggestions as proposed by members of the intermediaries interviewed in the survey:

- Intermediaries should play a preventive role against content offences but should not be held liable;
- There should be a systematic process in proving the intent of the intermediaries in giving consent or allowing content offences to take place;
- A clarification should be made about the wording "intentionally" and "false information," which overlap with Section 14 of the law;
- A committee or taskforce should be set up to help protect online intermediaries in litigation;
- If a trial takes place, there should be an injunction to protect intermediaries, possibly as witness; and
- Adaption or partial emulation of substance and implementation procedure of the US Digital Millennium Copyright Act (DMCA) is recommended.

G. Impacts on Content Regulation After Announcement of Martial Law and the July 2014 Coup

Since the staging of the coup on May 22nd, 2014 and the enforcement of martial law prior to that, the Thai political and communications sector have been markedly affected. Insofar as online intermediaries are concerned, the impacts can be analyzed from the vantage point of two groups of providers, based on first-hand assessment, as follows.

1. Network and Access Providers

Large network providers appear to be the ones suffering the least from the change in political regime. To them, the most evident impact is the increased burden in blocking websites. However, since this is carried out under an existing scheme of content filtering, the task has been quite manageable. Moreover, network providers that are state enterprises feel that they are obliged to support the policy of the coup makers, which, to them, signifies a much-needed intervention for the sake of the country. Likewise, the state-owned provider that has a content monitoring and filtering system in place has been cooperating fully with the new authority in surveillance and censorship of content offences or misdeeds against the NCPO in the online sphere. But for a privately owned network provider, the intervention of the coup means harder and more tedious work. With more rules and regulations, political content that was not classified as an offence before has become forbidden and has risen to top priority in the block list.

As for access providers, the assessment of the post-coup impact is quite similar to network providers although with more misgivings, as most of the access providers are private enterprises. Apart from shouldering a bigger burden in blocking websites, these providers have been compelled to keep pace with new announcements of the NCPO that are related to their operation, assign more staff to do round-the-clock patrolling of the network, and attend meetings with different authorities, including the NBTC and MICT. A foreign-owned access provider voiced the opinion that, despite their objection to the NCPO's blocking scheme that came in place of the court orders of the past, they are not in a position to defy it. Although they could clearly see the unfairness in blocking certain websites, they have had to comply and reserve their judgment.

2. Content Providers

The situation is quite different for content providers, particularly those that deal with political content and user-generated content. Two online newspapers and one web portal had to close down an interactive section for readers' comments, and the operator of an online discussion forum has been forced to remove an unprecedentedly high number of postings from the political discussion board. As a result, the scope of political discussions has become very limited and constrained. While the operator wishes to keep the forum open so that people would have space for exchange and release of political tension, people have become reluctant to participate because of the high level of censorship and the climate of fear. In addition, this operator has also tightened up the self-regulation scheme enforceable through the website's online community to guard against objectionable materials.

Meanwhile, the operator of a Facebook page for an online newspaper admitted that a much more meticulous process has been introduced to filter content prior to publication. All news, articles and commentaries must refrain from criticism of the NCPO to avoid being shut down. The basic rule is to stick to the facts, and avoid opinions and comments. Therefore, self-censorship has become the mantra of the day.

For those content providers with no interactive function, the impact has been quite minimal but they still proceed with much care. Two online investigative reporting websites reported that their news production and workflow had not been much affected, but they had to exercise extreme caution in choosing topics for investigation and in wording political content. For those specialty websites, electronic commerce, and web portals that have no bearing on politics, the only tangible impact is that there are more users and greater traffic than ever before. This is attributed to the fact that the spaces for political exchange and dialogue have shrunk, so websites that appeal to human interest have taken over in prominence.

V. Conclusion

On the one hand, the wording in Section 15 of the Thai computer crime law may be enough to exercise a chilling effect on every online intermediary. On the other hand, one prosecution after seven years does sound like a track record of leniency on the part of law enforcement. Intermediary liability in Thailand is indeed more complex than it seems for many reasons.

First, the structure of the Internet industry still contains viable remnants of state ownership and control from the past. While the survey data may not be all telling due to the need to comply with the interviewee's anonymity requirements, major Internet service providers in Thailand largely comprises of state enterprises, private corporations that have thrived on government concessions since the 1990s, and new players that came after the frequency reform in the mid-2000s. Within this context, these dominant players have been well disciplined to cooperate with the state's Internet regulation scheme that favors surveillance and censorship.

Over the course of the past two decades, a culture of censorship has gradually been established in which the Ministry of ICT is highly instrumental. Since this culture has been breeding an air of control and co-optation with the state, the emergence of the computer crime law and the provision on intermediary liability did not seem to represent a major change or pose a major threat to these operators. So long as they are disciplined partners with the state on content-related

issues complying with the culture of surveillance and censorship, they will not be targets of intimidation and control under the new law.

Unfortunately, such is not the case with the new wave of Internet content providers or online service providers that focus on providing content, as well as spaces where users can generate content on an open and participatory architecture of Web 2.0 Internet platforms – blogs, online forum, social networking services, among others. In the context of Web 2.0 communications, online content intermediaries have become important agents of control. So, governments – democratic and dictatorial – are passing on the censorship and surveillance role to these agents, whether they like it or not. The grave concern expressed and the real impacts felt by the studied content intermediaries after the May 2014 coup reflect the tremendous challenges facing this sector of intermediaries, who are generally smaller and less endowed with resources than the network and access providers to consistently cope with demands of the authority to guard against objectionable content.

Secondly, laws and the market regulate the Internet consistent with prevailing norms in Thailand, particularly ones that are inherent and socially shaping, like reverence for the monarchy. This is clearly reflected in the only case of intermediary liability prosecution involving the *Prachatai* online discussion forum. Not only does *Prachatai* represent a new wave of online content intermediaries that are markedly different from the conventional network and access providers as mentioned above, but *Prachatai* also represents a dissident online medium, since much of the website's content reflects progressive thinking and advocacy for changes from the status quo. And, perhaps it is for this reason that *Prachatai* was chosen to be an exemplar of the chilling effects of the computer crime law in the Thai Internet landscape.

It must not be forgotten that the charges filed against *Prachatai* covered both intermediary liability and lèse majesté, which is a severe offense in Thailand. The lèse majesté offence is also indicative of the underlying norms and values in Thai society – reverence of the monarchy and intolerance of criticism. This largely explains why local media or critics have not been very vocal in advocating for the cause of free expression in the trial of *Prachatai*'s web forum moderator. While free speech is high on the priority list of mainstream media in Thailand, *Prachatai* was not viewed as part of the group warranting such protection. As an alternative online media accused of breaching a draconian law, the case has slipped from the public eye. In effect, intermediary liability was superseded and overshadowed by lèse majesté, and the conventional and dominant understanding about what constitutes the media.

Nevertheless, the looming chilling effects caused by the intermediary liability provision are still real and made even more real by the recent change of political regime, and the unprecedented curbing of people's free expression. To recap, NCPO issued a couple of announcements targeting dissemination of information via online social media.

Overall, since the recent coup the mode of regulation for online intermediaries has shifted markedly from self-regulation to top-down sanction through an ad hoc body – the CSOC – that operates in a highly command and control fashion. The governance mechanism has also shifted from a criminal liability approach, as would be the case under the computer crime law, to upfront prior restraints associated with surveillance and censorship schemes. These constraining mechanisms appear to be more ex ante rather than ex post.

Under coup-shaped conditions, it is viable that coup announcements – which are equivalent to laws – have prevailed over other regulatory elements – market, code, or social norms – in the governance of Thai cyberspace. In this unusual and often regarded as temporary context, freedom of expression is not viewed necessarily as a crime, but more as something that needs to be curbed for the good of the country in its transitory path towards national reform.

Appendix F:
Turkey (eBay Case)

NoC Online Intermediaries Case Studies Series: Turkey (eBay Case)

Nilay Erdem and Yasin Beceni
BTS & Partners

Editorial Note: Context, Character, and Purpose of the Case Study

This case study is part of a globally coordinated, independent academic research project by the Global Network of Interdisciplinary Internet & Society Research Centers (NoC). Facilitated by the Berkman Center for Internet & Society at Harvard University, the project is the first output of a larger policy-oriented research initiative that examines the rapidly changing landscape of online intermediary governance at the intersection of law, technology, norms, and markets. In concert with other research projects, it seeks to develop criteria, comparative methods, and a shared data repository, and to compile insights and lessons learned across diverse communities of knowledge aimed at informing and improving Internet policy-making globally.

The initial research output consists of a case study series exploring online intermediary liability frameworks and issues in Brazil, the European Union, India, South Korea, the United States, Thailand, Turkey, and Vietnam, and a synthesis paper that seeks to distill key observations and provide a high-level analysis of some of the structural elements that characterize varying governance frameworks, with a focus on intermediary liability regimes and their evolution.

The authors of these case studies have participated in a multi-step process of in-person consultations and remote collaborations among a global team of researchers from the Network of Centers. Additionally, the case studies are based on a set of broader questions regarding the role of online intermediaries in the digital age.[1]

The research effort is grounded in a diversity of global perspectives and collaborative research techniques, committed to objective and independent academic standards, and aspires to be useful, actionable, and timely for policymakers and stakeholders. More broadly, the Network of Centers seeks to contribute to a more generalized vision and longer-term strategy regarding the role of academic research, facilitation and convening, and education and communication in the Internet age. For additional information on the initiative, please contact Urs Gasser, Berkman Center for Internet & Society, at ugasser@cyber.law.harvard.edu

[1] The process is documented at: "Online Intermediaries: Functions, Values, and Governance Options", The Global Network of Internet & Society Research Centers, 2014 https://drive.google.com/file/d/0B_ToTBKP5ITVWTl0UzV0U3B2RlU/view?usp=sharing.

Abstract: This case study provides an analysis and evaluation of the situation for online intermediaries in Turkey, with a focus on the problems faced by eBay after it acquired www.gittigidiyor.com, which was operating with a similar business model in Turkey. Within the scope of this case study, the online intermediary ecosystem and legislative environment in Turkey are first examined and then the above-mentioned eBay Case is analyzed in detail. The study concludes that basic problems for online intermediaries in Turkey are a result of the lack of proper legislation, and the government's attempts to suppress and control the Internet and online intermediaries in Turkey. Furthermore, Turkish courts' lack of understanding of online intermediaries' business models may cause those courts to render faulty decisions. However, despite these negative aspects, Internet usage and activities of online intermediaries in Turkey continue to grow.

Table of Contents

I. Introduction

This case study examines the challenges of e-commerce platforms in Turkey with a focus on problems faced by eBay after its acquisition of the company that owns www.gittigidiyor.com ("Gitti Gidiyor"), which operates according to an identical business model in Turkey. Before the discussion of Gitti Gidiyor, this study will first explain the online intermediary ecosystem in Turkey, mapping the general intermediary landscape and its legislative environment. After that, the study will review the eBay case in detail.

In 2011, eBay acquired Turkey's leading third party e-commerce platform, Gitti Gidiyor. EBay operates in Turkey under Gitti Gidiyor and no separate eBay entity exists in the market. Therefore eBay does not directly face problems in Turkey, but experiences difficulties through Gitti Gidiyor.

II. General Overview of the Online Intermediaries Ecosystem in Turkey

A. Internet Usage

Internet use in Turkey is increasing day by day. With its dynamic and young population of more than 76 million, and improved Internet infrastructure and mobile penetration, Turkey has one of the highest Internet usage rates in the world. According to the official statistics agency of Turkey (Turkish Statistical Institute),[2] the 2013 Internet access rate for businesses was 90.8%, while the same rate in households was 49.1%. According to the data published by the World Bank[3] in 2013, 46.3% of the Turkish population has access to the Internet and Turkey is ranked 93rd in Internet access rates in the world.

B. Ecosystem of Online Intermediaries

When we look at the ecosystem of online intermediaries, the main actors seem to be social media platforms and e-commerce websites. The table below shows the main providers by intermediary type:

Intermediary Type	International	National
Internet Search Engines	Google, Bing, Yahoo!, Yandex	-
Micro Blogs	Twitter	takiplen, democratus, peplr, freelyshout
Application Platforms	AppStore, iTunes, Google Play, Windows Store, Windows Phone Store, Nokia	-

[2] TurkStat, Use of Information and Communication Technology (ICT) in Enterprises, Use of Information and Communication Technology (ICT) in Households and Individuals (16-74 age group)

[3] The World Bank, based on the data gathered from the International Telecommunication Union, World Telecommunication/ICT Development Report and database, and World Bank estimates.

	Ovi Store, Blackberry World, Samsung Apps	
Social Media	Facebook, Pinterest, Foursquare, LinkedIn, Instagram, Flickr, Google+, Vine,	Hocam, quup, friendplans, feedfloyd, curbaa, esosyal, duube
User Generated Content Platforms	YouTube, Dailymotion, Vimeo	izlesene, ekşisözlük, itusözlük, incisözlük, 59 Saniye
E-Commerce Platforms	eBay, Amazon, asos,	Gitti Gidiyor (EBay), Kliksa, hepsiburada, Sahibinden Markafoni,

Figure 1. *Main intermediaries in Turkey*

International and national intermediaries currently dominate the Turkish market, and national intermediaries are generally imitations of international entities and are often not as popular as their international counterparts.

Currently, Turkey is witnessing an explosion in its citizens' use of online social media networks. It ranks 7th globally in the usage of Facebook and 10th for Twitter.[4] 93% of Turkish Internet users have Facebook accounts. Twitter follows Facebook with a usage rate of 72%, Google+ with a rate of 70%, LinkedIn with a rate of 33%, and Instagram with a rate of 26%. Currently, there are approximately 32,500,000 Facebook users in Turkey, approximately 41.59% of the population.[5] These rankings have made social media a powerful rival to the country's mainstream media. "Facebook is the most popular social network in Turkey", according to Social Bakers, "but recently Twitter and personal blogs have gained in popularity. Turkey's mobile penetration is larger than Internet penetration, which means that people increasingly access their social networks from mobile phones."[6] Furthermore, social media is heavily used for advertising purposes both by companies and politicians, as well as in social responsibility projects.

Within the context of e-commerce, Turkey's e-commerce sector generated approximately 7 billion USD per year as of 2012 and it is expected to grow 15.8% every year until 2017.[7] Online shopping is very popular among Turkish people and it is expected to gain more popularity over time. Women and young people buy items online much more than other segments of society.

[4] Common Ground of Digital Markets E-Commerce: Place of Turkey in the World, Current Situation and Steps for the Future, Turkish Industry and Business Association, July 2014, Accessible via: http://www.tusiad.org/__rsc/shared/file/eTicaretRaporu-062014.pdf

[5] Global Web Index Wave 11

[6] http://businessculture.org/southern-europe/business-culture-in-turkey/social-media-guide-for-turkey/ 03.12.2014

[7] Common Ground of Digital Markets E-Commerce: Place of Turkey in the World, Current Situation and Steps for the Future, Turkish Industry and Business Association, July 2014, page 35, Accessible via: http://www.tusiad.org/__rsc/shared/file/eTicaretRaporu-062014.pdf

Although Turkey's e-commerce market is not as developed as the United States or the European Union, it has great potential to grow.

Turkish society uses the Internet intensely; however, all services that are available in the US and the EU are not available in Turkey. For example, Turkish citizens cannot currently obtain e-books from Google Play Store or the Apple App Store. The same situation exists for Google's music and film services, as well as some of Google Maps' features.

Generally speaking, Turkish usage tendencies of social media are similar to the rest of the world considering that most Turkish users use social media to stay connected with friends, share comments and photos, and keep up with the news and current events. Furthermore, social media websites such as blogs, Facebook, and Instagram are also used for the sale of second hand things. However, there is a cultural difference when it comes to matchmaking websites. Many people who use dating websites are searching for "serious relationships" or "marriage," rather than a causal relationship. However, similar to the US, Turkish matchmaking websites target different demographics, with some tailored for religious people, lawyers, doctors, etc.

Twitter is a controversial but extremely popular social network in Turkey; in recent years, it has been one of the most-used tools for political and social expression. For instance, the Gezi Park protests of May and June 2013 showed an unexpected and extraordinary face of Turkish youth, a generation largely raised during a period devoid of widespread protests. This protest was largely motivated by the distribution of photos on social media that demonstrated a disproportionate use of force by police. Photos of their peers resisting water cannons and tear gas further inspired young people to join the protest. A micro blogging web site (delilimvar.tumblr.com) specifically aimed at protesters enabled them to report any excessive use of force by police. While most individuals who joined the demonstrations were not members of any political or social organization, social media allowed these previously non-activist youth to connect with each other. Additionally, protestors used social media to access information about the current situation in specific areas of the city where protests were planned. Likewise, individuals spread the contact information of lawyers and doctors available for aid over Facebook and Twitter.

The public reaction before the local election on March 30, 2014 is also illustrative of the use of Twitter for political and social expression. Before the election, an investigation into big corruption broke out in response to videos circulated on YouTube. The government immediately banned many YouTube links, but they couldn't block the spreading of Twitter links, which provided a new way to reach the public. In particular, citizens have found Twitter's "retweet" function to be especially useful to create public awareness during elections. After such developments, the ability of social media to allow people to express their opinion and organize for street protests was widely recognized by the government, academia, NGOs, and society itself.[8]

[8] Prof. Dr. B. Bahadır Erdem, Turkish Citizenship Law, 3rd Edition, Beta Yayıncılık, İstanbul, 2013, p. 76; An Examination of Gezi Park by Alternative Informatics Association, https://www.alternatifbilisim.org/wiki/Gezi_Park%C4%B1_De%C4%9Ferlendirmesi 26.09.2014

Turkish people often also use social network intermediaries like Facebook and Twitter to find blood and marrow for people who need them.[9] Many Internet celebrities will retweet or share requests for blood or marrow donation to spread them. The use of social media in such a way both creates public awareness for people in need, and generally increases blood and marrow donation rates.

LinkedIn, another international intermediary, has been popular in Turkish business life. Lots of people use LinkedIn to connect with business contacts and advance their career, find new job opportunities, as well as monitor friends and competitors.

YouTube and video websites are popularly used for watching old episodes of TV series, among other uses. Additionally, some professionals organize live business meetings on YouTube using the live stream feature.

As noted, some national intermediaries – imitations of international intermediaries such as Facebook and Twitter – are unsuccessful in Turkey. On the other hand, there are a couple of successful national intermediaries that have either copied an international concept by combining this concept with local cultural elements (such as underlying the privacy aspects of the site, providing additional payment options such as payment at the delivery, etc.); or have developed a fully national concept. In the field of e-commerce intermediaries, national intermediaries are more successful because of the trust relationship between website and user. The following paragraphs provide a couple of examples of successful national intermediaries in Turkey.

C. National Intermediaries

The most important of the successful Turkish intermediaries is "ekşisözlük". The name means "sour dictionary," but it is not a dictionary in the strict sense because, though the site defines words and/or terms, users are not required to write correct definitions. Ekşisözlük is not only utilized by thousands for information-sharing on various topics ranging from scientific subjects to lifestyle issues, but is also used as a virtual socio-political community to communicate disputed political content and to share personal views.

Ekşisözlük is an open area to express opinions, but also it has strict rules for entries and selecting writers. Writers are selected based on their draft entries, so the site aims to achieve a high intellectual level. Despite this aim, ekşisözlük has been losing its intellectual capacity, and is becoming a more and more politicized platform. Most of the users are in the opposition against the government but there are also a high number of users that are pro-government. It is currently one of the biggest online communities in Turkey with over 400,000 registered users and about 54,000 writers. However, the platform had only approximately 10,000 writers a couple of years ago, and therefore it was a much more of a boutique platform at that time, as it could be considered a more closed community because of stricter membership rules and content management.

---

[9] Although most of announcements are made individually, some of the Facebook groups are as follows (announcements repeatedly takes place on trend topic list of Twitter also): https://www.facebook.com/kanhayattir?fref=nf https://www.facebook.com/groups/kanaraniyor/?ref=ts&fref=ts https://www.facebook.com/iliknakli?ref=ts&fref=ts 03.12.2014.

The founders of ekşisözlük do not allow "troll" users, banning fake users or users who do not follow the rules of platform. Because of this kind of "high intellectual level" perspective, some people found this platform pretentious, establishing another platform – "incisözlük" – as a reaction. After the popularity of ekşisözlük, many similar social media platforms popped up but have not became as popular as ekşisözlük or incisözlük. incisözlük is popular for its anarchic attitude and having no active administration to select and screen writers. However, while it still has a moderation system – like ekşisözlük – for the content, incisözlük allows the users to write about almost any type of content (e.g. pornographic, daily life, etc…), without any limitation or format restrictions. The website represents different sub-cultures that have grown in Turkey since the 2000s. Sarcasm, parodies of clichés, and hatred of intellectualism on ekşisözlük have made incisözlük nearly as popular as ekşisözlük.

Turkish intermediaries such as ekşisözlük and incisözlük are similar with Wikipedia in the way that they are sources of information. However, while Wikipedia is much more like an encyclopedia and aims to provide objective information on historic or scientific facts, ekşisözlük and incisözlük are much more focused on daily events such as political issues, football games, or other such developments. In addition to those current events, ekşisözlük and incisözlük also contain information on historic and scientific facts, like Wikipedia. However, ekşisözlük and incisözlük are much more dynamic (new entries are provided by users nearly every minute of the day) than Wikipedia.

Another successful national intermediary is Hocam, a social media platform like Facebook intended only for college students who live in Turkey. Students can share their videos or photos, as well as create social groups or events. Just as Facebook was structured at the beginning, Hocam users can only sign up if they are university students. Both Hocam and another Turkish social media platform, quup, are very similar to Facebook. However, while Hocam has achieved significant popularity, quup is not popular. Quup's failure can be explained by its content management strategy. Quup is a social media platform, but it does not host content created by the users. Rather, it only hosts content created by the editors, fetched from newspapers, magazines, etc. Hocam's success can be attributed to its unique theme and restricted member acceptance policies, explained above.

59saniye is a user generated content platform on which users can share or broadcast every kind of video as long as it is less than 59 seconds. Such a duration cap makes the site attractive for people who do not have lots of time to watch long videos or who do not like long videos. The motto of the website is "'cause 1 minute is too much time," further demonstrating this intermediary's concept.

Another rising trend that allows new national intermediaries to flourish is e-commerce. For Turkish citizens, trust in e-commerce platforms is rising constantly, thereby increasing the opportunity for online shopping. Many e-commerce websites popped up after reinforcing their security measures and the numbers of online shoppers is increasing constantly as a consequence. The most popular national intermediaries that host e-commerce platforms are Markafoni, Trendyol, hepsiburada, sahibinden, kliksa, and n11.

III. Governance and Responsibility Mechanisms

A. Overview of Internet Governance in Turkey

Online intermediaries in Turkey are not treated differently within the framework of Internet governance in Turkey. In other words, all online intermediaries, without any classification regarding sector or services provided, are accepted as hosting providers and thus are subject to the Law numbered 5651 on Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting (here after referred to as the "Internet Law"), which went into force on May 4th, 2007. Per the Internet Law, hosting providers are defined as real persons or legal entities that provide or run systems that contain services and content. Therefore, all online intermediaries running systems that contain services and content are considered *hosting providers*, and are not responsible for checking the hosted content or whether the content constitutes an unlawful activity, pursuant to the Internet Law. This being said, they shall remove illegal content, provided that they have been informed about the illegal content.

With the increase in the volume of Internet users in Turkey, important amendments were made to the Internet Law in February 2014 in order to adapt the law to the latest changes in technology and compound the liabilities of content, hosting, and service providers. The amendments have been heavily criticized by academics, NGOs, and society and it is claimed that the amendments are aimed at suppressing and controlling the Internet, granting unlimited authority to administrative bodies, and violating individuals' freedom of expression and right to privacy.[10] One of the amendments made to the Internet Law relates to the categorization of hosting providers. Accordingly, hosting providers, within the scope of the principles and procedures to be determined by secondary regulation, may be categorized based on the nature of their business and be differentiated in respect to their rights and liabilities. As seen in this clause, though, online intermediaries are not categorized based on the nature of their business in the present time, though they may be classified in that way in the future since the Internet Law leaves a space in this respect.

Another important document that supports the categorization of hosting providers is the Draft 2014-2018 Information Society Strategy and Action Plan of Turkey ("hereinafter referred to as Draft Action Plan"), which was formulated by the Ministry of Development and which designates the strategies and actions to be followed by 2018. One of the strategies determined in the Draft Action Plan is the "certification of e-commerce websites." Being considered within the scope of the definition of hosting providers, e-commerce websites shall be subject to a certification process in order to provide secure shopping experiences for customers. As per the Draft Action Plan, the minimum standards for e-commerce websites must be determined by 2016 and the certificates will be given to those e-commerce websites meeting the standards. In addition to that, the e-commerce websites that do not meet the minimum standards shall be sentenced to sanctions to be determined, and a dynamic accreditation infrastructure shall be established in order to regularly audit the activities of those sites. If the actions in the Draft Action Plan are realized, this may create positive results for online intermediaries because a certification system will prove that the website is safe to use, hence users may abandon their safety-based hesitations. Also, other goals stated in the Draft Action Plan, such as the generalization of Internet access, strengthening the Internet infrastructure, and enhancing the

[10] Kerem Altıparmak, Yaman Akdeniz "An Examination of the Draft Amendments on Law No. 5651" http://cyber-rights.org.tr/docs/5651_Tasari_Rapor.pdf 25.09.2014

quality of human resources can be very beneficial to online intermediaries both in their internal operation and their expansion in the Turkish market. Subject to the liability clauses of the Internet Law, the players in the telecommunications sector in Turkey are also subject to regulations prepared by the Information and Communications Technologies Authority, a technically independent organization still controlled by the Ministry of Transport and Communications.

B. Regulations Effecting E-Commerce Ecosystem

The effect of the Turkish Regulatory environment on online intermediaries can be grouped into two different categories, considering their method of application. These are: (i) regulations directly applicable to the online intermediaries, and (ii) general rules and regulations which are applied to online intermediaries in certain events.

1. Regulations Directly Applicable to the Online Intermediaries

The first group of the regulations, which are directly applicable to online intermediaries, consist of the above mentioned Internet Law,[11] the Law Governing E-Commerce, the Framework on the Taxation of E-Commerce, the E-Archive Regulations, the Draft Law on Data Protection, the Law on the Payment and Securities Reconciliation Systems, the Payment Services and Electronic Money Institutions (the "E-Money Law"), and the Consumer Protection Law.

i. The Law Governing E-Commerce

The Law Governing E-Commerce numbered 6563 was reviewed and accepted by the General Assembly of Turkish Grand National Assembly on October 23rd, 2014 and published in the Official Gazette on November 5th, 2014, numbered 29166. According to the Law, its provisions are enforceable on May 1st, 2015. The Law Governing E-Commerce regulates the roles and responsibilities of e-commerce service providers, intermediary service providers, and electronic commercial communications. The E-Commerce Law explicitly states that intermediaries are not under any obligation to control the legality of the content or sales of goods provided by the users of the platform. The E-Commerce Law also stipulates that the application of the requirements regarding informing the users, sales, and electronic commercial communication will be determined by secondary regulations. The aforementioned provision has the potential to provide additional protection for intermediaries from secondary liability.

The E-Commerce Law is expected to be beneficial for intermediaries since it will regulate specifically the non-liability of intermediaries. Therefore the E-Commerce Law may solve the problems of intermediaries in cases where the courts hold them liable.

ii. Taxation of E-Commerce

Taxation of e-commerce in Turkey is based on the OECD's "Electronic Commerce: Taxation Framework Conditions" report, which was accepted by Council of Ministers in 1998. This report is significant, setting the basic principles for implementation of e-commerce taxation to international transactions. Many countries, including Turkey, are setting their national practices accordingly. Additionally, the Revenue Administration of the Ministry of Finance has published

[11] Since the Internet Law is one of the main topics of this study and has been discussed in other sections.

a framework regarding the responsibilities of e-entrepreneurs in relation to the application of taxation rules to e-commerce activities[12].

Most recently, the Revenue Administration published the Communiqué of the Tax Procedural Law numbered 433 on December 30th, 2013 in order to provide an e-archive invoice application to enable the electronic storing of invoices issued electronically, as well as enable B2C e-invoicing. According to the Communiqué, taxpayers that have garnered revenue of more than 5 million Turkish Liras as of 2014 must start using the e-archive invoicing application before 2016. The Communiqué of the Tax Procedural Law numbered 433 is very beneficial to online intermediaries because it allows digitalization in fiscal matters, which is a field with significant paper work.

iii. Data Protection

Turkey has no specific law governing the privacy of personal data. Nonetheless, there is a Draft Data Protection Law, and there are general provisions in relation to privacy and personal data protection in a number of pieces of legislations. There are some sector-based regulations in place for the telecommunications, banking, insurance, capital markets, and health sectors as well.

According to the Constitution, the right to personal data protection shall ensure that the data subject has the right to be informed about the processing of his/her personal data, others' access to that data, requests for the data's correction and deletion, and if the data is being used for the related purpose or not. The same article also states that personal data may only be processed under circumstances stated by law or under the explicit consent of the data subject. There are also punitive provisions set forth in the Turkish Criminal Code. Additionally, there are provisions of the Turkish Civil Code that give individuals whose personal rights are unjustly violated the right to file a civil action.

However, none of these regulations create a clear framework for the protection of personal data. The current Draft Data Protection Law is based on the EU 95/46/EC Data Protection Directive and requires explicit consent of the data subject both for processing personal data and for transferring the personal data to third parties and/or abroad, unless the processing falls under the scope of the Law's exceptions. Absent a framework, data protection is causing problems in the data flow to Turkey, since Turkey is considered an unsecure country by EU data protection authorities. Therefore, it is nearly impossible to conduct data based activities in Turkey from abroad.

Furthermore, companies often cannot sufficiently plan their path of operation because they cannot predict when the Draft Data Protection Law will be enacted. This uncertainty generally results in personal data programs being run in accordance with the Draft Data Protection Law. However, amendments to the Draft Data Protection Law and future regulations pursuant to the law will eventually require the modification of personal data compliance programs, which means additional costs for companies, including intermediaries.

---

[12] Çağatay Pekyörür, Nilay Erdem, Selen Uğur, Tugrul Sevim, Yasin Beceni, "Electronic Commerce and Taxation", published article on "Vergi Sorunları Dergisi" ("Peer-Review Taxation Issues Journal"), Issue 293, February 2013

Without a data protection law, personal data does not have sufficient protection, which creates doubts in the public about the usage of online intermediaries. Therefore, online intermediaries' growth is jeopardized by the absence of a data protection law.

iv. E-Money Law

The E-Money Law was published in the Official Gazette dated June 27th, 2013, numbered 28690 and became effective as of the date of its publication. The Law aims to regulate payment systems, payment services, and electronic money services, and sets forth the principles and procedures with regard to the establishment, authorization, and operation of the providers. According to the Law, payment service providers and e-money institutions should obtain licenses from the Banking Regulation and Supervision Authority in order to continue their activities in Turkey. One of the most challenging provisions for foreign players of such a law is the local information systems requirement. In order to obtain the necessary license, payment service providers and e-money institutions must keep their primary and secondary IT systems within the borders of Turkey.

v. Law on Consumer Protection

The new Law on Consumer Protection, which replaces the Law numbered 4077 on Consumer Protection, was enacted by the Turkish Parliament on November 7th, 2013 and will be effective six months after its publication in the Official Gazette.

According to the Consumer Protection Law, in the case of a distance contract, the consumer has the right of withdrawal within 14 days without paying any kind of penalty and without stating a reason.

Additionally, the Consumer Protection Law stipulates that the intermediaries with distance contracts should keep records of transactions between sellers and buyers, and should provide such information to the relevant institutions and customers when asked. Such intermediaries are responsible to sellers and buyers in accordance with their contractual relationship. In this clause, intermediaries with distance contracts have limited liability under these contracts, and cannot be held liable for the execution of the distance contract itself because their role is limited to that of an intermediary, and therefore they are not a party to the distance contract.

3. General Rules and Regulations Applied to Online Intermediaries in Certain Events

Furthermore, a second group of regulations exist, consisting of real-world legislation, including customs regulations, the Draft Communiqué on V.A.T., the Regulation on Importation, Production, Process and Presentation to the Market of Food Supplements, and the Regulation on Debit and Credit Cards. In certain cases, such regulations have been applied directly to intermediary platforms or to the users of such platforms based on the type of marketed goods, the V.A.T applied to the sale, or fraudulent activity performed on the platform.

The Ministry of Finance has been drafting a new Communiqué (the "Draft Communiqué") to merge all communiqués regarding the VAT. The Draft Communiqué includes provisions that extend the application scope of the VAT at auction places by including bargains and other types of sales that shall cause VAT. Such a Communiqué may result in additional liability for the intermediaries that have business models based on auctions.

The Regulation on Importation, Production, Process, and Presentation on the Market of Food Supplements stipulates that food operators shall register websites and URL addresses to local offices of the Food and Control General Directorate of the Ministry of Food, Agriculture, and Livestock. Accordingly, the Regulation permits the sale of food supplements via registered URLs and stipulates fines for food operators who act against such provisions. Therefore, in order to market food supplements through intermediaries, sellers must register their URLs at intermediaries' platforms in accordance with the Regulation.

Additionally, according to the new amendments to the Regulation on Debit and Credit Cards, offering payments with installments through credit cards is limited to nine installments (including the period of deferral of payments) in general and such service cannot be offered for the purchases of food, fuel, or for expenses related to telecommunications or jewelry. This amendment put an additional burden on intermediaries to control the sales on their platform in order to categorize goods that may fall under the payment with installments prohibition.

C. Main Governance Mechanisms

Regulators use both *ex ante* and *ex post* mechanisms in order to regulate online intermediaries. The *ex ante* instrument used by the government to regulate online intermediaries is the operating certificate issued by the Telecommunications Authority. Per the Regulation Regarding Principles and Procedures for Granting Operating Certificate to Access and Hosting Providers by Telecommunications Authority, all types of access and hosting providers shall be required to obtain operating certificates. Since online intermediaries are considered hosting providers in Turkey, before providing services they must apply to the Telecommunications Authority and obtain operating certificates.[13] Without such a certificate, the service provided by the online intermediaries shall be suspended. In other words, the operating certificate is the instrument enabling online intermediaries to provide services in accordance with the law. However, foreign online intermediaries that do not have a local entity in Turkey are excluded from the burden of obtaining the certificate because they are out of jurisdiction of Turkey.

In addition to that, the *ex post* mechanism described in the Internet Law also regulates online intermediaries. The provisions under the Internet Law try to balance the rights of the users and those who claim that their rights have been violated through the websites. Considering the proportionality principle, the Internet Law allows for URL blocking rather than blocking entire websites (excluding exceptional cases).[14] Accordingly, in a case where the right of a user is violated, only the web page containing the related content shall be removed; thus, the users will be able to continue their activities on the other pages of the related website.

IV. Liability

[13] Article 4 paragraph 1 of the Regulation Regarding Principles and Procedures for Granting Operating Certificate to Access and Hosting Providers by Telecommunications Authority

[14] As per Article 8 paragraph 1 of the Internet Law, access to an entire website on the Internet may be blocked if there is sufficient suspicion that the content constitutes crimes which are provocation for committing suicide, sexual harassment of children, easing the usage of drugs, supplying drugs which are dangerous for health, obscenity, prostitution, providing place and opportunity for gambling; and crimes mentioned in the Law on Crimes Against Atatürk dated 25.07.1951 and numbered 5816.

A. Liability Framework

Pursuant to the Internet Law, "hosting providers who do not make the hosting provider notification or do not fulfill the obligations determined by this Law shall pay an administrative fine anywhere from 10 thousand Turkish Liras to 100 thousand Turkish Liras by the Presidency."[15] In light of this clause, online intermediaries that do not remove illegal content from broadcast once they have been informed about that content shall be fined.

Online intermediaries also become liable when they do not remove illegal content after being informed of its existence in the cases in which the content constitutes defamation, violation of trademark protection, or violation of copyright protection.

1. Defamation

As per the Turkish Criminal Code, any person who acts with the intention to harm the honor, reputation, or dignity of another person is sentenced to imprisonment from three months to two years, or forced to pay a punitive fine. The content can possibly be evaluated under article 125 of the Criminal Code and the person may be charged with committing a "defamation" crime.

2. Personal Right Violations

Additionally, Turkish Civil Code designates personal rights violations. Since the right to protect one's honor and dignity is deemed a personal right, content violating honor and dignity may be deemed a personal rights violation as well. In the event of a personal rights violation, the complainant may file a lawsuit to request the termination of the violating material, the removal of the violating thread, the examination of the content, material indemnification, moral indemnification, and/or material compensation from the violator. In regards to violations over the Internet, in practice rights holders obtain preliminary injunctions from courts for blocking access to websites on which the violating content is available. Several courts decisions have led content to be blocked from a number of different websites.

It also should be noted that the actual practice in Turkey with regards to Internet content is still vague and the application of it by different judicial authorities varies. Although blocking access is a procedure that is specifically designated for a limited number of circumstances, the authors of this case study have still observed in practice that some courts may grant blocking access decisions for content for which such decisions cannot be legally made accordance with the Internet Law.

3. Crimes Against Ataturk

Moreover, Turkey has a specific law on crimes against Ataturk (Mustafa Kemal Atatürk, the founder of modern Republic of Turkey) called the Law on Crimes against Ataturk, numbered 5816 dated 25/7/1951. According to Law no 5651 on the Regulation of Broadcasts via the Internet and the Prevention of Crimes Committed through such Broadcasts, Internet sites that include content that can sufficiently be considered to constitute a crime under the Law on Crimes against Ataturk may be subject to blocking. As such, websites like Youtube can be blocked because of defamation against Ataturk. As sufficient suspicion of this crime can directly result in a blocking access decision, reports claiming defamation against Ataturk should be handled in a

[15] Article 5, paragraph 6 of the Internet Law

careful and prompt manner. Since the matter is delicate in terms of national values and sensitivities, interpretation of was constitutes "defamation against Ataturk" is wide. For example, content showing Ataturk in make-up and as a woman; remarks about Ataturk's sexuality; remarks about Ataturk being a womanizer or drunk all carry the risk of being deemed defamatory and therefore risk prompting a blocking access decision.

The most well known case of blocking access to a website due Crimes against Atatürk was a series blockings to YouTube between March 2007 and October 2010. The first blocking was due a video on YouTube that insulted Atatürk. This ban was removed after the content was removed from the website. Between 2008 and 2010, YouTube was blocked continuously by a couple of court orders due to Crimes Against Ataturk.[16]

4. Copyright Protection

Copyright protection is granted under the Law no. 5846 on Intellectual and Artistic Works ("FSEK"). According to FSEK, in the case of a copyright violation over the Internet, natural or legal persons whose rights have been violated shall initially contact the content provider and request that the violation cease within three days. Should the violation continue, a request should next be made to the public prosecutor, who will require that the relevant ISP suspend the service provided to the content provider in question within three days. The service provided to the content provider shall be restored if the violation ceases. Please note that Law no 5846 does not define content provider. In practice, in addition to actual content providers, blocking access decisions against hosting providers can also be handed down pursuant to this provision. MySpace and Last FM are examples of websites that have been blocked pursuant to this provision.

5. Additional Regulations

In addition to these provisions that specifically set forth a blocking procedures, Turkish courts and judges have in the past the granted blocking-access decisions based on various other regulations, including:

- Turkish Civil Law
- The Law on Combat Against Terrorism
- Actions that may constitute a crime in accordance with "Turkish Criminal Law" (especially for web sites which publish content about sensitive political issues in Turkey, such as Kurdish issue, Armenian issue, etc)

Please note that those pieces of legislation do not designate a specific blocking procedure. However, the courts did grant blocking decisions pursuant to these regulations, as well as based on temporary measures such as preliminary injunctions for personal rights violations pursuant to Turkish Civil Law. In recent decisions of the Court of Cassation, the Internet Law is a specific

[16] Alper Çelikel, Blocking Access to Youtube.com from Turkey and Its Consequences from the Perspective of Freedom of Expression, 2011, https://www.academia.edu/1937347/YOUTUBE.COM_WEB_SITESINE_TURKIYEDE_ERISIMIN_ENGELLENMESI_VE_IFADE_HURRIYETI_BAKIMINDAN_SONUCLARI 26.09.2014

regulation compared to the Turkish Civil Law and is therefore applicable to personal rights violations on the Internet.[17] After that decision, courts started to apply only the Internet Law.

In addition to that, if online intermediaries do not maintain and update their indicative information accurately and completely on their own sites in a way that the users can access directly from the main page, they can pay an administrative fine of two thousand to ten thousand Turkish Liras.

B. Safe Harbors

According to the Internet Law, since online intermediaries are not responsible for checking hosted content or researching whether the content constitutes an unlawful activity, online intermediaries are not liable in cases where they are not informed of the infringing content. This being said, per the Internet Law, intermediaries can be "informed" via any channel considered to be contact information under the law. In other words, the Internet Law does not designate a specific channel to contact online intermediaries about such violations.

Upon notification in accordance with the Internet Law, online intermediaries have to remove the content. Before the February 2014 amendments to the Internet Law, online intermediaries' responsibility for removing the content was limited by technical possibilities (i.e. sufficient technologies to remove the content); however, the February 2014 amendments removed the technical possibilities limitation from the Internet Law. Online intermediaries will be punished with administrative fines in the amount of 10,000.00 TRY to 100,000.00 TRY if they do not remove content that they have been properly notified about.

As explained above, the E-Commerce Law provides a safe harbor for online intermediaries by establishing that they are not liable for third party content. However, until the E-Commerce Law is enforceable, judicial and administrative bodies cannot apply it.

C. Enforcement

Before the amendment to the Internet Law, the users who claimed that their rights have been violated through websites were first obliged to apply to the online intermediary in question in order to ask for the removal of the content. The amendment to the Internet Law has changed this "notice and take down*"* procedure and gives two options to users. Accordingly, users whose rights have been violated may apply to the content/hosting provider for the removal of the content, or can directly bring a lawsuit against the content provider. In other words, with the amendments to the Internet Law the "notice and take down*"* procedure has been evolved to a procedure of "notice/no notice block." This amendment weakened online intermediaries' power to apply their terms of use or other policies and to consider disputes themselves. Most Turkish users prefer to apply to courts rather than intermediaries. Since the courts do not have a sufficient understanding of such disputes, online intermediaries sometimes have to remove the content or block access in Turkey unfairly. Furthermore, online intermediaries have to be very quick to

[17] Court of Cassation, 4th Section of Law, Case No: 2012/2045, Decision No: 2013/1218, Decision Date: 29.01.2013. (In Turkish: Yargıtay 4. Hukuk Dairesi, E. 2012/2045, K. 22013/1218, T. 29.01.2013) http://66.221.165.113/cgi-bin/highlt/ibb/highlight.cgi?file=ibb/files/4hd-2012-2045.htm&query=5651%20Say%FDl%FD%20Yasa%20%F6zel#fm

respond to such requests because the Internet Law establishes a period of only a couple of hours for trial and enforcement proceedings.

According to the legal procedure stipulated in the Internet Law, any real person, legal entity, institution, or entity who claims that his/her personal rights have been violated may either:

- Apply to the content/hosting provider for its removal. There is no specific limitation about the method of communicating with the content/hosting provider, so the user's application to the intermediary by filling out the reporting form would constitute a "warning to the content/hosting provider" as per the Internet law, or
- Go directly to the court and request for the URL blocking to the specific content. The court may also order blocking of the entire website if the violation cannot be stopped otherwise.

D. Significant Cases

On March 21st 2014, Twitter was banned in Turkey because of three court orders and a public prosecutor's request regarding the removal of content. Since Twitter is one of the most popular social media websites in Turkey, the reactions against the blocking order spread on media in a very short time. Thus, in order restore access to Twitter, personal applications were made to the Constitutional Court of Turkey. On April 2nd, 2014, the Constitutional Court of Turkey stated that the TA should enforce the order immediately and ruled that such a general ban on Twitter was a violation of freedom of expression. The Constitutional Court also noted in its order that since the Internet Law provides for URL blocking, blocking access to the whole website violates the proportionality principle.[18] After this order, the Twitter ban was removed.

One week after the Twitter ban, on March 27th, 2014, YouTube was also banned due to the presence of a voice recording of a meeting of high officials, including the Foreign Affairs Minister, the Undersecretary of National Intelligence Service, and the Deputy Chief of Staff of Turkish Armed Forces. The decision stated that contents in 15 URL addresses would be removed unless access to YouTube was fully blocked. Following the blocking order, many applicants, including YouTube, applied to the Constitutional Court claiming that blocking access to the website violated their constitutional rights.

On June 13th, 2014, the Constitutional Court ruled that blocking access to YouTube constituted a violation of freedom of expression.[19] The decision of the Constitutional Court first explained freedom of expression in the scope of the constitution and human rights. In addition, the court stated that the Internet has great value for the exercise of fundamental rights and freedoms, especially for freedom of expression. Social media is now indispensable for persons to express, share, and promulgate their knowledge and opinions. Therefore, per the Constitutional Court, it is explicitly clear that the government and administrative institutions have to act responsibly while regulating the Internet and social media instruments, which have become the most effective methods of self-expression. Furthermore, the Constitutional Court ruled that there is

[18] Constitutional Court, Application No. 2014/3986, Decision Date: 02.04.2014, http://www.resmigazete.gov.tr/eskiler/2014/04/20140403-18.pdf 26.09.2014
[19] Constitutional Court, Application No. 2014/4705, Decision Date: 29.05.2014 http://www.resmigazete.gov.tr/eskiler/2014/06/20140606-10.pdf 26.09.2014

nothing in the Internet Law that allows for blocking access to an entire website instead of conducting URL blocking or blocking with other methods that constitute a lighter-touch intervention. Therefore, the Telecommunications Authority did not have the authority to completely block access to YouTube, and the ban violated fundamental rights and freedoms of the applicants.

V. eBay Case Study

A. Information About eBay and Gitti Gidiyor

eBay, founded in San Jose, California in 1995, is the world's biggest online marketplace. It facilitates users buying and selling items in almost every country worldwide, and has made advances in digital marketing, multi-channel retail, and global e-commerce. In addition, eBay reaches millions of people through StubHub (the world's biggest online marketplace for tickets) and job posting sites that cover more than 100 cities around the world. The company is based in the US and operates as a limited liability company listed in the NASDAQ stock exchange. eBay has 97 million users and, as of 2013, was worth $212 billion.

eBay Inc. owns a series of third party e-commerce platforms worldwide, platforms where sellers exhibit their goods for sale online, as well as provide secure payment between the parties of such sales. eBay's role is limited to providing a platform to bring together buyers and sellers; it does not engage at any point in online retail activity and does not make any legal transactions as a buyer or a seller.

In 2011, eBay acquired 93% of the shares of Turkey's leading third party e-commerce platform, Gitti Gidiyor, which operates an identical business model in Turkey. The deal followed eBay's acquisition of a minority stake in Gitti Gidiyor in 2007.

Gitti Gidiyor was established as a company with three partners in 2001. It has more than 10 million registered users and more than 27 million visitors (with 12.5 unique visitors) per month. On average, 750,000 sales take place on the site each month, which corresponds to 1 sale every 3 seconds. The total number of sales transactions that have taken place on the site is more than 30 million.[20]

Gitti Gidiyor is a platform that provides a secure payment and communication service to its users who are carrying out e-commerce transactions. The role of a third-party marketplace platform, such as the one operated by Gitti Gidiyor, is to create a trusted online environment where buyers and sellers can trade goods and services among themselves. Gitti Gidiyor is not an online retailer, but merely hosts content created by others. The users of Gitti Gidiyor, in addition to creating the content themselves, carry out transactions on the online platform without any involvement of the company itself. Users do not involve the company at any stage of the sales and, further, Gitti Gidiyor is not a party to the sales agreement. One of the main features of Gitti Gidiyor is its "Zero Risk" payment system. The "Zero Risk" payment system aims to provide a safe method of payment for online transactions, where the rights of both the sellers and purchasers are protected during the process of delivery and examination of the product.

[20] These numbers are abstracted from the information on Gitti Gidiyor's website at http://www.gittigidiyor.com/hakkimizda/tarihce.

B. Challenges for eBay as an Intermediary Operating in Turkey

In certain cases, Gitti Gidiyor is deemed liable – just like the actual perpetrator of a crime or an infringer – for the unlawful acts conducted on the platform and/or in relation to the products sold on its platform. Some examples of such liability problems are as follows.

1. Challenges Related to Customs Issues

Since it is not possible for Gitti Gidiyor as a hosting provider to see, know, or evaluate the exact nature or origin of the goods traded by its users, Gitti Gidiyor has no legal or criminal liability in relation to the goods that are sold or offered for sale on its platform. Gitti Gidiyor is recognized as a "hosting provider" under the Internet Law by the Information and Communication Technologies Authority's (ICTA) Telecommunications Directorate. As explained above, according to the Internet Law hosting providers like Gitti Gidiyor have no responsibility to check the content that they are hosting or to proactively investigate whether their users are breaking the law.

Despite the fact that Gitti Gidiyor as an intermediary has no control over or knowledge of the transactions carried out by buyers and sellers through its platform, certain Customs Enforcement Directorates have held Gitti Gidiyor liable for breaches of Anti-Smuggling Law No. 5607 ("Law No. 5607") through an interpretation based on the assumption that Gitti Gidiyor acts as a mediator in the sale of smuggled products by users on its platform.

Law no 5607 Article 3 includes an exhaustive list of acts deemed to be "Smuggling Acts," which does not include "acting as a mediator in the sales of smuggled goods." In addition to the fact that the law does not include such an act on its exhaustive list, it is not Gitti Gidiyor but the buyers and the sellers who carry out the transactions on the platform by reaching an agreement about the sale price, characteristics, and delivery conditions of the product. It is without a doubt that Gitti Gidiyor is not a party to such sales contracts between the related buyers and sellers. Therefore, Gitti Gidiyor should not be held liable under Law No. 5607.

In a case regarding Law No. 5607, a customs enforcement directorate made a complaint to the public prosecutor and requested that he press charges against Gitti Gidiyor, claiming that Gitti Gidiyor was helping its users to commit smuggling crimes. After the investigation, the public prosecutor filed a case to a criminal court. These claims were rejected by the court[21] for the reason of the non-liability of Gitti Gidiyor as an intermediary. However, the court did not specifically reference the Internet Law, which regulates the non-liability of the hosting providers. Instead, the court stated that it was impossible for Gitti Gidiyor to control all the products sold through its platform, and it therefore cannot be held liable from a criminal law perspective, since it did not commit a negligent act.

2. Challenges Related to V.A.T. Liabilities

The Ministry of Finance is drafting a new Communiqué (the "Draft Communiqué") to merge all communiqués regarding the VAT. The Draft Communiqué includes provisions that extend the scope of the VAT at auction places by including bargains and other types of sales that shall cause

[21] Criminal Court of First Instance, Hatay, Case No: 2011/1030, Decision No: 2012/595, Decision Date: 18.04.2012, approved by the decision of the Court of Cassation, 7th Section of Criminal Department, Case No: 2013/21432, Decision No: 2014/12444, Decision Date: 18.06.2014

VAT. It is not clear whether e-commerce intermediaries that provide financial and commercial activities to others will be deemed auction-style platforms, or whether such intermediaries will be deemed auction-holders.

3. Challenges Related to Sales of Products

The sale of products of a specific nature is another issue for platforms like Gitti Gidiyor. Such products of a specific nature are pharmaceutical products, tobacco and alcohol, food supplements, guns and firearms, historical artifacts, etc. E-Commerce platforms tend to ban the sale of such products and they also use technical tools to avoid such sales. However, because many people use such platforms and many transactions are realized on them, it is easy to miss single sales or offerings. Turkish authorities have the tendency to initiate actions against e-commerce platforms in relation to such sales or offerings without first notifying the platform about the issue and asking for removal.

C. Impact Assessment of the Challenges

The problems of eBay-Gitti Gidiyor in Turkey have mainly resulted from the lack of understanding in Turkey about the principle of "non-liability of intermediaries" provided that they meet certain obligations. One of the other reasons for the problems is the fact that it is more difficult to find the actual the perpetrators of a crime if such a crime is committed online. As finding such actual perpetrators is difficult, the administrative and judicial authorities tend to hold Gitti Gidiyor liable for issues related to its platform. Be it customs, V.A.T., advertising, or distance sales, the main reason for problem is the fact that authorities in Turkey tend to deem hosting providers (or intermediaries, in international terminology) liable and/or try to sanction them for actions and/or content on the platform that they are providing.

In addition to being contrary to the principle that a platform like Gitti Gidiyor cannot be held criminally or otherwise liable for the activities of the users, as laid down in European Union harmonized legislation, as well as the corresponding legislation in Turkey, the misinterpretation of the Law No. 5607 could have far-reaching negative consequences for the development of e-commerce in Turkey, and for much-needed local and foreign investment in this field. Problems with the V.A.T. liabilities and sales of products are another example of how an e-commerce business model may be treated the same as the actual provider of a service and expected to meet the same requirements as such parties.

The above problems caused by a lack of understanding of the non-liability principle hamper the growth of the online intermediaries in Turkey and damage the willingness of the foreign online intermediaries to enter into the Turkish market. Furthermore, these problems concern users, as it appears online intermediaries may be conducting illegal activities and therefore may be dangerous to use. As can be seen, this lack of understanding has many negative effects on online intermediaries.

D. Recommendations/Solutions in Light of the eBay Case

As mentioned, the above problems result from the fact that an intermediary non-liability regime is not clearly imposed in the judicial and administrative environment of Turkey. In light of this finding, our recommendations are:

- Turkey should closely follow the developments of policy, strategy, and action plans, as well as the legislation, of countries where e-commerce is developed and Turkish authorities should clearly understand the ratio legis (the reason of enacting the law) behind such documents, in particular regarding the non-liability of e-commerce platforms.

- The regulations and policies to be implemented by the Ministry of Customs and Trade's Internal Trade General Directorate (the organ given authority by the E-Commerce Law) in relation to newly enacted E-Commerce Law, which clearly imposes the non-liability for e-commerce platforms, will be of high importance.

A structure should be established where public authorities think and act in cooperation with private sector representatives and civil society when making or amending policies and legislation.

Legislation on e-commerce may solve most of the problems intermediaries are facing, especially in the field of liability. The previously mentioned structure is a key element to monitoring international development, and therefore it may significantly effect e-commerce legislation. It appears that the above mentioned elements are connected and must be applied in combination to achieve success.

VI. Conclusion

Our studies of online intermediaries in Turkey show that Internet usage is spreading in the country and the society is at the beginning of exploring the potential of the Internet in the economy, politics, socialization, and charitable action. Within this exploration process, national intermediaries – both imitations of international online intermediaries such as Facebook and Twitter, and unique ones – are beginning to flourish in the country. Also, society is beginning to use online intermediaries in different ways and is eager to expand both the usage of the Internet and these platforms. It should also be stated that despite the government's unsupportive statements towards social media, social media usage is continuing to rise due people's need to communicate and express their opinions. Consequently, it is widely expected that Internet usage will continue to spread across the country, and therefore online intermediaries will gain more and more popularity in the future. This will cause inevitable changes in the economy, politics, and social life in the near future.

Although people are generally willing and eager to use the Internet and online intermediaries, the legislative and administrative environments are somewhat hostile towards both the Internet and online intermediaries. Government efforts to control and suppress the Internet and online intermediaries have not been successful so far due people's willingness, technical impossibilities, and court decisions. However, these efforts have caused a loss in prestige for the government internally and externally. Furthermore, the absence of data protection laws and e-commerce laws is an obstacle facing the development of online intermediaries in Turkey. The government's unwillingness to enact the above mentioned laws – combined with its efforts to control and suppress of Internet – have been heavily criticized. Taxation problems and credit card installment limitations are other problems that online intermediaries are facing that are directly affecting them economically. Although these may be justified by referencing the public interest, such as

reducing the current deficit and increasing tax income, these problems are damaging the growth of online intermediaries in Turkey.

An important aspect of the Internet Law is its requirement for online intermediaries to obtain operating certificates. Operating certificates allow the government to know who owns and controls the online intermediary, and apply the law (when necessary) directly to this owner, as well as conduct communications regarding the government's requests through the provided contact information. However, while operating certificates may seem a tool of control for the government, they have a benefit for online intermediaries in that they prove the owner is a hosting provider and therefore not responsible for the content it hosts. Another control mechanism of the government is the ability to block access to websites. Although this is not a precise solution since a block can easily be circumvented, it allows the government to force intermediaries – especially foreign intermediaries – to obey Turkish law and court orders.

The liability of online intermediaries is mainly regulated under the Internet Law and a couple of other laws that include relevant provisions. Although the Internet Law accepts that online intermediaries are not responsible for the content that is created by their users, there are problems with this aspect of the law, in that the courts do not always accept it. Furthermore, the access blocking mechanism causes damage to online intermediaries even though they are not responsible for the content. Therefore it can be said that the online intermediary is forced to control the content created by its users even though it cannot be punished pursuant to the law. Moreover, there is no obligation for the applicant to notify the online intermediary before removing content. The website of the online intermediary can be blocked even without the knowledge of the online intermediary.

In the eBay-Gitti Gidiyor case, the effects of the unawareness of the principle of non-liability of online intermediaries can be easily seen. Challenges faced by Gitti Gidiyor in customs, product sales, and taxation clearly show that administrative and judicial authorities in Turkey are not applying the principle correctly. Given Turkey is a developing country with a young population – which means it is a huge market for online intermediaries – misconduct of administrative and judicial authorities affects society in many ways. This study recommends that the application and quality of the current legislation should be improved by cooperation of public institutions, the private sector, and NGOs.

Bibliography

Legislation

Anti-Smuggling Law No. 5607 (*Published in the Official Gazette dated March 31st, 2007 and numbered 26479*)

Communiqué of the Tax Procedural Law numbered 433(*Published in the Official Gazette dated December 30th, 2013 and numbered 28867*)

Constitution of the Republic of Turkey (*Published in the Official Gazette dated November 9th, 1982 and numbered 17863*)

Consumer Protection Law (*Published in the Official Gazette dated November 28th, 2013 and numbered 28835*)

Draft Communiqué on V.A.T. (*Pending at Revenue Administration to be enacted*)

Draft Data Protection Law (*Pending to be presented to the Parliament*)

Law no. 6563 Governing E-Commerce (*Published in the Official Gazette dated November 5th, 2014 and numbered 29166*)

Law no. 5846 on Intellectual and Artistic Works (*Published in the Official Gazette dated December 13th, 1951 and numbered 7981*)

Law numbered 5651 on Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting (*Published in the Official Gazette dated May 23rd, 2007 and numbered 26530*)

Law on Crimes Against Atatürk (*Published in the Official Gazette dated July 25th, 1951 and numbered 5816*)

Law on the Payment and Securities Reconciliation Systems, the Payment Services and Electronic Money Institutions (*Published in the Official Gazette dated June 27th, 2013 and numbered 28690*)

Regulation on Debit and Credit Cards (*Published in the Official Gazette dated December 17th, 2010 and numbered 27788*)

Regulation Regarding Principles and Procedures for Granting Operating Certificate to Access and Hosting Providers by Telecommunications Authority (*Published in the Official Gazette October 24th, 2007 and numbered 26680*)

Turkish Civil Code (Published in the Official Gazette dated December 8th, 2001 and numbered 24607)

Turkish Criminal Code (*Published in the Official Gazette dated October 12th, 2004 and numbered 25611*)

Court Decisions

Court of Cassation, 4th Section of Law, Case No: 2012/2045, Decision No: 2013/1218, Decision Date: 29.01.2013.

Criminal Court of First Instance, Hatay, Case No: 2011/1030, Decision No: 2012/595, Decision Date: 18.04.2012 (*approved by the decision of the Court of Cassation, 7th Section of Criminal Department, Case No: 2013/21432, Decision No: 2014/12444, Decision Date: 18.06.2014*).

Constitutional Court, Application No. 2014/3986, Decision Date: 02.04.2014, http://www.resmigazete.gov.tr/eskiler/2014/04/20140403-18.pdf

Constitutional Court, Application No. 2014/4705, Decision Date: 29.05.2014 http://www.resmigazete.gov.tr/eskiler/2014/06/20140606-10.pdf.

Articles and Reports

AFRA, Sina. "Common Ground of Digital Markets E-Commerce: Place of Turkey in the World, Current Situation and Steps for the Future," Turkish Industry and Business Association, July 2014.

Pekyorur, Erdem, Ugur, Sevim, Beceni. "Electronic Commerce and Taxation," Vergi Sorunları Dergisi" ("Peer-Review Taxation Issues Journal"), Issue 293, February 2013.

"Electronic Commerce: Taxation Framework Conditions," OCED, Report by the Committee on Fiscal Affairs, as presented to Ministers at the OECD Ministerial Conference, "A Borderless World: Realizing the Potential of Electronic Commerce" on 8 October 1998.

Prof. Dr. B. Bahadır Erdem, "Turkish Citizenship Law," 3rd Edition, Beta Yayıncılık, İstanbul, 2013

Online Resources

GittiGidiyor. "About Us." http://www.gittigidiyor.com/hakkimizda/tarihce.

Global Web Index. "Wave 11." https://www.globalwebindex.net/.

The World Bank. "Internet Users (per 100 people)." http://data.worldbank.org/indicator/IT.NET.USER.P2.

TurkStat. "Use of Information and Communication Technology in Enterprises." http://www.turkstat.gov.tr/PreTablo.do?alt_id=1048.

Alternative Informatics Association. "An Examination of Gezi Park." https://www.alternatifbilisim.org/wiki/Gezi_Park%C4%B1_De%C4%9Ferlendirmesi.

Kerem Altıparmak, Yaman Akdeniz. "An Examination of the Draft Amendments on Law No. 5651." http://cyber-rights.org.tr/docs/5651_Tasari_Rapor.pdf.

Alper Çelikel. "Blocking Access to YouTube.com from Turkey and Its Consequences from the Perspective of Freedom of Expression." 2011. https://www.academia.edu/1937347/YOUTUBE.COM_WEB_SITESINE_TURKIYEDE_ERISIMIN_ENGELLENMESI_VE_IFADE_HURRIYETI_BAKIMINDAN_SONUCLARI

Appendix G:
Intermediary Liability in the United States

NoC Online Intermediaries Case Studies Series: Intermediary Liability in the United States

Adam Holland, Chris Bavitz, Jeff Hermes, Andy Sellars, Ryan Budish, Michael Lambert, and Nick Decoster
Berkman Center for Internet & Society

Editorial Note: Context, Character, and Purpose of the Case Study

This case study is part of a globally coordinated, independent academic research project by the Global Network of Interdisciplinary Internet & Society Research Centers (NoC). Facilitated by the Berkman Center for Internet & Society at Harvard University, the project is the first output of a larger policy-oriented research initiative that examines the rapidly changing landscape of online intermediary governance at the intersection of law, technology, norms, and markets. In concert with other research projects, it seeks to develop criteria, comparative methods, and a shared data repository, and to compile insights and lessons learned across diverse communities of knowledge aimed at informing and improving Internet policy-making globally.

The initial research output consists of a case study series exploring online intermediary liability frameworks and issues in Brazil, the European Union, India, South Korea, the United States, Thailand, Turkey, and Vietnam, and a synthesis paper that seeks to distill key observations and provide a high-level analysis of some of the structural elements that characterize varying governance frameworks, with a focus on intermediary liability regimes and their evolution.

The authors of these case studies have participated in a multi-step process of in-person consultations and remote collaborations among a global team of researchers from the Network of Centers. Additionally, the case studies are based on a set of broader questions regarding the role of online intermediaries in the digital age.[1]

The research effort is grounded in a diversity of global perspectives and collaborative research techniques, committed to objective and independent academic standards, and aspires to be useful, actionable, and timely for policymakers and stakeholders. More broadly, the Network of Centers seeks to contribute to a more generalized vision and longer-term strategy regarding the role of academic research, facilitation and convening, and education and communication in the Internet age. For additional information on the initiative, please contact Urs Gasser, Berkman Center for Internet & Society, at ugasser@cyber.law.harvard.edu

[1] The process is documented at: "Online Intermediaries: Functions, Values, and Governance Options", The Global Network of Internet & Society Research Centers, 2014 https://drive.google.com/file/d/0B_ToTBKP5ITVWTl0UzV0U3B2RlU/view?usp=sharing.

Abstract: This paper describes and assesses the intermediary liability landscape in the United States. It provides an overview of major US legal regimes that protect online intermediaries in cases where third-parties seek to hold them liable for the conduct of their users, addressing both the Digital Millennium Copyright Act safe harbor enshrined in Section 512 of the United States Copyright Act and Section 230(c) of the Communications Decency Act. It then offers a series of case studies describing ways in which US-based companies and other organizations have structured their operations in compliance with and in response to US law. The paper describes Craiglist's response to efforts to hold it responsible for sex trafficking that occurred on the site; the ContentID copyright and VERO trademark programs implemented by YouTube and eBay, respectively; and the reactions of intermediaries to allegations of wrongdoing by Wikileaks. It provides an assessment of the importance of transparency reporting for online intermediaries as they seek to address tensions between requirements of legal compliance and the need to secure users' trust. And, it concludes with a detailed and thematically-organized literature review that summarizes the state of scholarship in this space.

Table of Contents

I. Introduction

The United States offers a unique and interesting case, from both a legal and policy perspective, for study of the governance landscape for online intermediaries. This is true for at least two major reasons.

First, the US is the birthplace of, and home to, many major global Internet platforms that host content and make this content available to users. It is thus unsurprising that US law incorporates significant protections for such online intermediaries in cases where third parties seek to hold them liable for the conduct of their users. At the same time, the US is also home to a significant and robust content industry that has played a major role in shaping its intellectual property – particularly copyright – regimes. The tension between content owners (who place a premium on preventing infringement of the content that drives their traditional business models) and intermediaries (which require immunity from third-party claims in order to avoid crippling financial liability) raises fundamental questions about the role of government and the prioritization of business interests.

Second, US law provides robust protections for speech, rooted in the First Amendment to the United States Constitution. Government-sanctioned restraints on speech – particularly prior restraints imposed without significant consideration to due process – are very strongly disfavored under US law. A court order requiring that a piece of content – e.g., a blog post or image or video – be removed from an online platform implicates the free speech rights of the person who created that content. State and federal legislatures crafting laws (and courts applying and interpreting them) must consider the rights of that speaker, along with the rights of the subject of the speech in question and the role of the intermediary, in crafting appropriate remedies.

This paper offers a short legal primer describing the two major provisions of federal law – the "Digital Millennium Copyright Act" or "DMCA", and the safe harbors embodied in Section 512 of the United States Copyright Act and Section 230(c) of the "Communications Decency Act" or "CDA" – that govern liability and immunity of online intermediaries in the United States, and the common law provisions that fill gaps not addressed by these two statutory regimes. After mapping the landscape for intermediary liability in the US, the paper turns to a series of case studies that highlight how a range of actors in various sectors of the Internet ecosystem have grappled with intermediary liability concerns in addressing their business and related needs. These case studies demonstrate both the importance and the limitations of existing intermediary liability regimes and the creative ways in which companies and others have worked within (and around) existing law to allocate liability in ways that work for them. Finally, the paper turns to a discussion of the role of transparency for intermediaries attempting to balance the competing interests described above and the need to maintain positive relationships with both the public and their user base.

II. Legal Landscape Primer

A. General Content Liability

1. Traditional Defamation Liability for Intermediaries

Publishing a false factual statement about a person that harms their reputation can lead to a civil

(and, extremely rarely, criminal[2]) claim of defamation.[3] Defamation has a complicated structure; the tort evolved from the common law of the individual states, with a series of United States Supreme Court cases adding some specific, nationwide carve-outs and requirements deemed to be necessary in light of the First Amendment.[4] The law still varies considerably across each state, but to make out a claim of defamation today a plaintiff generally needs to show, among other things, (1) that a defendant published a statement; (2) that the statement was a false statement of fact (as opposed to true facts or an opinion); and (3) that the defendant acted with a certain level of fault (depending on the person involved, either negligence or "actual malice," a term of art roughly meaning the defendant knew the statement was false at the time it was published).[5]

Claims against content intermediaries need to satisfy these elements as well, but any party against whom all of the elements of a defamation claim exist is potentially liable.[6] Prior to the advent of the Internet, courts limited the universe of possible defendants by requiring that an intermediary only be held liable if they "know[] or ha[ve] reason to know" of the statement's defamatory character.[7]

This leads to different results based on different intermediaries in the offline world. Newspapers and magazines tend to be held responsible for their content, even when the content clearly owes its origin to a third party – e.g., with a letter to the editor.[8] The opposite result is usually reached when considering contract printing shops or "vanity presses."[9] Those who distribute or host physical copies of defamatory publications are usually protected for the same reason, and scholars openly question whether a library or bookseller could ever be held liable for distributing

---

[2] *See* David Pritchard, *Rethinking Criminal Libel: An Empirical Study*, 14 COMM. L. & POLICY 303, 313 (2009) (finding 2-9 prosecutions a year in the state of Wisconsin, but noting this to be significantly a significantly higher rate than commonly thought). The Media Law Resource Center reported no criminal defamation cases in 2013. *See New Developments 2013*, Media L. Resource Ctr. Bulletin 90 (December 2013).

[3] *See generally* http://www.dmlp.org/legal-guide/defamation.

[4] Robert C. Post, *The Social Foundation of Defamation Law: Reputation and the Constitution*, 74 CAL. L. REV. 691 (1986).

[5] Parties must also show that the statement was about the plaintiff and that the statement harmed the plaintiff's reputation. Most states also require a plaintiff to show that they suffered "actual damages" based on the statement, or that the statement falls into one of several categories where damages are presumed. *See Defamation*, DIGITAL MEDIA LAW PROJECT, http://www.dmlp.org/legal-guide/defamation (last updated Aug. 12, 2008). When discussing public officials and figures, the First Amendment case law requires a plaintiff to show that the defendant acted with "actual malice," a term of art meaning that the defendant knew the statement was false when they published it, or acted with reckless disregard of the truth. For more on private and public figures, see *Proving Fault: Actual Malice and Negligence*, DIGITAL MEDIA LAW PROJECT http://www.dmlp.org/legal-guide/proving-fault-actual-malice-and-negligence (last updated Aug. 7, 2008). There are other overlapping claims that may be asserted in conjunction with defamation, but they are usually confined to the same general requirements as to falsity and fault. *See Other Falsity-Based Legal Claims*, DIGITAL MEDIA LAW PROJECT, http://www.dmlp.org/legal-guide/other-falsity-based-legal-claims (last updated Aug. 15, 2008).

[6] Rodney Smolla, Law of Defamation § 4:87.

[7] RESTATEMENT (SECOND) TORTS § 581. This scienter requirement has now spread to all claims of defamation through Supreme Court precedent, but nevertheless serves as a useful heuristic for separating parties traditionally liable for defamation from those who were not. *See* Smolla, *supra* note [[x]], at § 4:92.

[8] Sack on Defamation § 7.1; Marc A. Franklin, *Libel and Letters to the Editor: Toward an Open Forum*, 57 U. COLO. L. REV. 651 (1986).

[9] Sack on Defamation § 7.3.4.

defamatory books, even if they had reason to know of the book's character.[10] Telegraph and telephone companies have generally been protected against claims for transmitting defamatory statements, though often with a stated exception for when the company knew of the message's defamatory nature.[11]

Radio and television stations are generally held responsible for pre-recorded content, but live broadcasting presents a curious analytical challenge, as the station may not have the time to harbor any knowledge of a statement's defamatory and false nature between when it is spoken and when it is aired.[12] At least one court has held that open solicitation of content without a broadcast delay system could lead to liability under a recklessness standard,[13] but most other courts take the opposite approach.[14]

Even when an intermediary publisher or conduit is held responsible for the content it is disseminating, other doctrines in defamation law provide protection to avoid inappropriate results. States adopt variations on a "fair report privilege," which allows for the fair and accurate republication of statements made in official public documents or proceedings.[15] Many states also provide a "wire service defense," which allows for the republication of defamatory content from a reputable news agency, provided the re-publisher did not know or have reason to know the information was defamatory and did not substantially alter the content.[16] Some states have also adopted a "neutral reportage" defense, to protect the republication of statements that are worthy of public discussion because they were made, even if the re-publisher believes them to be false – e.g., a wild allegation made by one politician against another during an election.[17] Such defenses, in particular cases, could extend to intermediaries hosting or republishing the content of others.

---

[10] Sack on Defamation § 7.3.4 ("Suppose a person were to inform public libraries and news vendors that a book, newspaper, or newsmagazine they are distributing contains false and defamatory statements . . . . May the libraries or vendors then be held liable for continuing to sell or circulate the offending material? That is possible, although the potential for use of that tactic to turn financially vulnerable distributors into censors . . . argues strongly for a complete distributors' immunity from suit."); Prosser and Keeton on Torts § 113 (1984) ("It would be rather ridiculous, under most circumstances, to expect a bookseller or a library to withhold distribution of a good book because of a belief that a derogatory statement contained in the book was both false and defamatory . . . ."); Loftus E. Becker, Jr., *The Liability of Computer Bulletin Board Operators for Defamation Posted by Others*, 22 Conn. L. Rev. 203, 227 (1989) ("[N]o one seems to have sued a library for defamation in this century."). For an example of a case that held a bookseller liable based on this theory, *see* Janklow v. Viking Press, 378 N.W.2d 875 (S.D. 1988); RESTATEMENT (SECOND) TORTS § 581 cmt. e (acknowledging possible liability for libraries and bookstores in exceptional cases).

[11] *See Liability of Telegraph or Telephone Company for Transmitting or Permitting Transmission of Libelous or Slanderous Messages*, 91 A.L.R.3d 1015 (1979) (citing numerous cases where courts applied the Restatement's knowledge requirement or found categorical immunity for telegraph and telephone companies). Courts acknowledge the policy reasons for giving telegraph companies the leniency in deciding whether they should have known that a dispatch was defamatory. Gray v. W. Union Tel. Co., 13 S.E. 562 (Ga. 1891); *but see* Paton v. Great N.W. Tel. Co., 170 N.W. 511 (Minn. 1919) (finding potential liability for telegraph company for transmission).

[12] *See* Sack on Defamation § 7.3.5.A.2.

[13] Snowden v. Pearl River Broad. Corp., 251 So. 2d 405 (La. Ct. App. 1971).

[14] Sack on Defamation § 7.3.5.A.2 n. 66 (gathering cases).

[15] *See Fair Report Privilege*, DIGITAL MEDIA LAW PROJECT, http://www.dmlp.org/legal-guide/fair-report-privilege (last updated July 22, 2008).

[16] *Wire Service Defense*, DIGITAL MEDIA LAW PROJECT, http://www.dmlp.org/legal-guide/wire-service-defense (last updated July 22, 2008).

[17] *See Neutral Report Privilege*, DIGITAL MEDIA LAW PROJECT, http://www.dmlp.org/legal-guide/neutral-report-privilege (last updated July 22, 2008); Sack on Defamation § 7.3.5.D.

In the early days of Internet's widespread adoption, commentators and cases sought to analogize re-publisher and distributor liability when considering bulletin boards and other online content platforms.[18] After one court assigned liability for the Internet service provider Prodigy Services Co. for content on one of its bulletin boards, based on the fact that Prodigy exercised general editorial control over the platform, Congress opted to define a different standard for online intermediary liability.[19]

2. Traditional Privacy Liability for Intermediaries

Privacy laws in the United States consist of a patchwork of common law torts and specific statutory enactments, overlaid with nationwide exceptions made in light of the First Amendment.[20] Intermediaries primarily concern themselves with privacy law to the extent it impacts their own businesses operations and practices – for example, how they represent their data handling practices to the public, and how they handle their own data security.

A second form of privacy liability for intermediaries stems instead from the actions taken on behalf of others, and whether the intermediary can ever be held liable for contributing (willingly or not) to those actions. The laws around such invasions of privacy can be generally clustered into two categories: those that address the unlawful gathering of information (e.g., intruding into one's private spaces or unlawfully recording conversations), and those that address publishing private information (e.g., the "public disclosure of private facts" tort or publishing specific information proscribed by statute[21]). The First Amendment plays a role in this space by both limiting the universe of defendants for intrusion claims[22] and by substantially limiting the types of claims that can be brought regarding the disclosure of private information.[23]

With respect to information gathering, many states recognize a tort called "intrusion upon seclusion," which punishes one who intrudes into the solitude or seclusion of another in a way that is highly offensive to a reasonable person.[24] Because the defendant's conduct usually must be intentional for liability to attach, it is rare to see liability extend to disinterested intermediaries.[25] At least one court has found secondary liability could attach to a newspaper for

---

[18] *See, e.g.*, Becker, *supra* note [[x]].

[19] *See* David Ardia, *Free Speech Savior or Shield for Scoundrels: an Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOYOLA OF L.A. L. REV., 373, 407-11 (2010) (chronicling the history of the lead-up to Section 230, including the Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995)).

[20] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 77 (3d ed. 2009).

[21] For an example of this, *see* 18 U.S.C. § 2710 (governing when and how a customer's video rental history may be disclosed).

[22] *See* notes [[x–y]], *infra*, and accompanying text.

[23] While the states that recognize a public disclosure tort include a definitional balance that precludes claims against newsworthy information, the Supreme Court has yet to directly consider a challenge to public disclosure torts in other cases. *See* Geoffrey R. Stone, *Privacy, the First Amendment, and the Internet*, in THE OFFENSIVE INTERNET (Saul Levmore & Martha C. Nussbaum eds. 2010). For more on the history of balancing between free speech and privacy has had a complicated century of history. *See* Geoffrey R. Stone, ANTHONY LEWIS, FREEDOM FOR THE THOUGHT THAT WE HATE 59-80 (2009).

[24] RESTATEMENT (SECOND) TORTS § 652B.

[25] *See, e.g.*, Marich v. MGM/UA Telecomm., Inc., 113 Cal. App. 4th 415 (2003) (defining intent for California's intrusion tort). For examples of cases where parties were liable as aiders or abettors of another's intrusion, *see* DAVID A. ELDER, PRIVACY TORTS § 2:9.

running a classified ad that facilitated intrusion of another, though in that case the plaintiff pleaded that the newspaper published the ad with the intent to invade the plaintiff's privacy.[26]

Some intrusion laws attempt to indirectly target intrusion by punishing those who later disclose or receive the information that was unlawfully acquired. But First Amendment doctrine prevents the application of such laws to those who did not actively participate in the unlawful acquisition, at least when the information is true and a matter of public concern.[27] This would seem to preclude most information intermediaries from liability for transmitting content that was unlawfully acquired by others.

Laws concerning the disclosure of private information directly can vary considerably, but most states have some form of the tort called "public disclosure of private facts," which concerns the intentional disclosure to the public[28] of non-newsworthy information about an individual that is highly offensive to a reasonable person.[29]

Unlike defamation or intrusion, the specific mental state of defendants varies considerably between states, so the *mens rea* does not generally limit liability for disinterested intermediaries in the same way as other torts.[30] That said, the few cases that consider a distributor's liability tend to impart the same requirement from defamation cases that the distributor know the information to be tortious in order to be held liable.[31] Also, information obtained from public sources are considered protected under the First Amendment,[32] and republishing content originally published widely by others does not lead to liability in most cases, as the fact that the content was published previously means that the information is no longer considered private.[33]

The traditional standards for intermediary liability in privacy are applied in a radically different manner online, in large part due to Section 230 of the Communications Decency Act, which is discussed in the following section.

3. Section 230 of the Communications Decency Act

As noted in the preceding sections, liability for offline content distributors or hosts largely turns on whether the host knows or has reason to know that they are hosting tortious content. In the

---

[26] Vescovo v. New Way Enters., Ltd., 60 Cal. App. 3d 582 (1976).

[27] *See, e.g.*, *Bartnicki* v. *Vopper*, 532 U.S. 514, 526 (2001) (The First Amendment prevents a radio broadcaster from being punished for disclosing the contents of an unlawfully-intercepted communication); Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 104 (1979); Food Lion, Inc. v. Capital Cities/ABC, Inc., 194 F.3d 505 (4th Cir. 1999) (refusing to escalate damages for breach of duty of loyalty based on subsequent disclosure of information); Doe v. Mills, 536 N.W.2d 824 (Mich. 1995) (knowing receipt of information unlawfully obtained does not lead to intrusion claim for the recipient). Scholars have been mindful to point out that the exact meaning and scope of the "*Daily Mail* principle" is not entirely clear. Janelle Allen, *Assessing the First Amendment as a Defense for Wikileaks and Other Publishers of Previously Undisclosed Government Information*, 46 U.S.F. L. REV. 783, 798 (2012).

[28] This is deliberately made a wider audience than defamation, for which liability attaches when a statement is "published" to a single person. RESTATEMENT (SECOND) TORTS § 652D cmt. a.

[29] RESTATEMENT (SECOND) TORTS § 652D.

[30] DAVID A. ELDER, PRIVACY TORTS § 3:7.

[31] *See, e.g.*, Steinbuch v. Hachette Book Grp., 2009 WL 963588 at *3 (E.D. Ark. April 8, 2009); Lee v. Penthouse Int'l Ltd., 1997 WL 33384309 at *8 (C.D. Cal. March 19, 1997).

[32] *See, e.g.*, The Florida Star v. B.J.F., 491 U.S. 524 (1989).

[33] *See, e.g.*, Ritzmann v. Weekly World News, 614 F. Supp. 1336 (N.D. Tex. 1985); Heath v. Playboy Enters., Inc., 732 F. Supp. 1145 (S.D. Fla. 1990); *but see* Michaels v. Internet Ent. Grp., Inc., 5 F. Supp. 2d 823 (C.D. Cal. 1998) (disclosure of more than the ways originally revealed in first publication can give rise to claim for republication).

earliest days of the Internet, courts used these standards to assess liability of online intermediaries, but found that the law created a perverse result. Online intermediaries possessed the technical ability to filter or screen content in the way an offline intermediary never could, but under existing standards this meant that the intermediary would assume liability for all the content over which they had supervisory control. In the most famous case on point, this included a service that was trying specifically to curate a family friendly environment, at a time when the public was greatly concerned about the adult content on the Internet.[34] In order to "to promote the continued development of the Internet and other interactive computer services and other interactive media [and] to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services," Congress enacted Section 230 of the Communications Decency Act.[35]

Section 230 prevents online intermediaries from being treated as the publisher of content from users of the intermediaries. By the terms of the statute, "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." [36] An "interactive computer service" under Section 230 is defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server . . . "[37] Online intermediaries of all sorts meet this definition, including Internet service providers, social media websites, blogging platforms, message boards, and search engines.[38] An "information content provider" in turn is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[39]

Section 230 covers claims of defamation, invasion of privacy, tortious interference, civil liability for criminal law violations, and general negligence claims based on third-party content,[40] but it expressly excludes federal criminal law, intellectual property law, and the federal Electronic Communications Privacy Act or any state analogues.[41] Its terms also specify that the coverage is for "another's" content, thus not protecting statements published by the interactive computer service directly.[42] Thus, to apply Section 230's protection, a defendant must show (1) that it is a provider or user of an interactive computer service; (2) that it is being treated as the publisher of content (though not with respect to a federal crimes, intellectual property, or communications privacy law); and (3) that the content is provided by another information content provider.

---

[34] Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). *See also* LAWRENCE LESSIG, CODE 2.0 249-52 (2006) (discussing the Internet anti-pornography efforts happening around the time of the Communications Decency Act debate).

[35] 47 U.S.C. § 230. The section was part of a greater law that sought to relegate the transmission of offensive content to minors, the majority of which was later struck by the Supreme Court. *See* Reno v. ACLU, 521 U.S. 844 (1997).

[36] 47 U.S.C. § 230(c)(1).

[37] § 230(f)(2).

[38] *See* Ardia, *supra* note [[x]], at 387-89.

[39] § 230(f)(3).

[40] *See* Ardia, *supra* note [[x]], at 452.

[41] § 230(e)(1)–(4). The Electronic Communications Privacy Act governs the voluntary and compelled disclosure of electronic communications by electronic communications services.

[42] *See* § 230(c)(1).

The law was designed in part to foster curation of online content, and courts have found that a wide array of actions can be taken by "interactive computer services" over third-party content are covered by Section 230. These include basic editorial functions, such as deciding whether to publish, remove, or edit content;[43] soliciting users to submit legal content;[44] paying a third party to create or submit content;[45] allowing users to respond to forms or drop-downs to submit content;[46] and keeping content online even after being notified the material is unlawful.[47] This applies to both claims rooted in defamation and those rooted in invasion of privacy.[48]

On the other hand, if the intermediary creates actionable content itself, it will be liable for that content.[49] Courts are also unlikely to find that Section 230 applies when an interactive computer service edits the content of a third party and materially altering its meaning to make it actionable;[50] requires users to submit unlawful content;[51] or if the service promises to remove material and then fails to do so.[52] When an intermediary takes these actions, it is deemed to have "developed" the content by "materially contributing to the alleged illegality of the conduct."[53]

While stated very simply, the law upsets decades of precedent in the areas of content liability law, and radically alters the burdens on online services for claims based on user content.[54] By limiting any assumed liability for a wide range of content-based claims (and given the other content areas discussed below), Section 230 effectively removes any duty for an interactive computer service to monitor content on its platforms, a tremendous boon for the development of new intermediaries and services.[55] Virtually all liability for content-based torts is pushed from the service to others, often the user. In practical terms, however, this has yet to manifest a windfall for online services; many claims are still brought against online intermediaries, and the

---

[43] *See* Donato v. Moldow, 865 A.2d 711 (N.J. Super. Ct. 2005).

[44] *See* Corbis Corporation v. Amazon.com, Inc., 351 F.Supp.2d 1090 (W.D. Wash. 2004); *see also* Global Royalties, Ltd. v. Xcentric Ventures, LLC, 544 F. Supp. 2d 929, 933 (D. Ariz. 2008) (holding that even though a website "encourages the publication of defamatory content," the website is not responsible for the "creation or development" of the posts on the site).

[45] *See* Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998).

[46] *See* Carafano v. Metrosplash.com, 339 F.3d 1119 (9th Cir. 2003).

[47] *See* Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997). Promising to remove content and then declining to do so, however, can expose an interactive computer service to liability. *See* Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009). For more examples of actions likely to be covered under Section 230, *see Online Activities Covered by Section 230*, DIGITAL MEDIA LAW PROJECT, http://www.dmlp.org/legal-guide/online-activities-covered-section-230 (last updated Nov. 10, 2011).

[48] *See, e.g.*, Jones v. Dirty World Entertainment Recordings, LLC, 2014 WL 2694184 (6th Cir. 2014) (defamation claim preempted by Section 230); Doe v. Friendfinder Network, 540 F. Supp. 2d 288, 302–303 (D.N.H. 2008) (intrusion upon seclusion and public disclosure of private facts claims preempted).

[49] *See* MCW, Inc. v. Badbusinessbureau.com, LLC, 2004 WL 833595, No. 3:02-CV-2727-G at *9 (N.D. Tex. April 19, 2004) (the operator of a website may be liable when it is alleged that "the defendants themselves create, develop, and post original, defamatory information concerning" the plaintiff).

[50] *See Online Activities Not Covered by Section 230*, DIGITAL MEDIA LAW PROJECT, http://www.dmlp.org/legal-guide/online-activities-not-covered-section-230 (last updated Nov. 10, 2011).

[51] *See* Fair Housing Council v. Roommates.com, LLC, 521 F.3d 1157, 1175 (9th Cir. 2008) (en banc).

[52] *See* Barnes v. Yahoo!, Inc, 570 F.3d 1096 (9th Cir. 2009).

[53] *See* Jones v. Dirty World Entertainment Recordings, LLC, 2014 WL 2694184 (6th Cir. 2014).

[54] *See* Ardia, *supra* note [[x]], at 411.

[55] *See, e.g.*, Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 1, 17 (2014) ("Section 230 immunity . . . ha[s] been among the most important protections for free expression in the United States in the digital age. [It] has made possible the development of a wide range of telecommunications systems, search engines, platforms, and cloud services without fear of crippling liability.").

question is often litigated extensively and at great expense before courts find that claims are invalid.[56]

As noted above, Section 230 does not cover intellectual property laws, and thus different rules apply in these cases. These are now addressed.

B. Copyright

1. A General Overview of Secondary Liability for Copyright Infringement

In U.S. law, copyright liability comes in two main forms, "primary" or "direct" liability, and "secondary liability".[57] The first, direct liability, is the liability that attaches to an actual infringer of the copyright(s) in question, whether by copying without authorization or by violating any of the other rights that copyright owners possess, as described in 17 U.S.C. 106 of U.S. law. Direct liability, although it can become more complex depending on the facts surrounding an alleged infringement, is generally quite straightforward. Either copyright was infringed or it wasn't.

The second type of liability, secondary liability, is more nuanced, in large part because there is nothing in U.S. copyright statute that expressly provides for such liability. Secondary liability in the United States is therefore what is known as "judge-made" law, a set of rules and guidelines, rising out of other areas of liability law[58], that have accumulated over time on a case-by-case basis, that then exist as binding precedent. This makes secondary liability more fact specific and also potentially more prone to evolve based on changes in technology and normative behaviors.[59]

Within this framework, secondary liability is conceptualized as taking on one of two forms[60]: that resulting from "vicarious infringement" and that resulting from "contributory infringement." Each version requires that there first be a direct infringement. The remaining differences are subtle but critical, especially with respect to the implicit incentives for potential secondary infringers, and address a potential secondary infringer's "knowledge" of any direct infringement, the degree to which the infringer has the ability to control the direct infringement, and their financial benefit, if any. Each of these facets are critical to understanding the competing imperatives that online intermediaries ("OI"s) face, and it is with respect to OIs that this section's further discussion will proceed.

---

[56] *Id.* at 493.

[57] There are mentions in the literature and case law of a concept of "tertiary liability, "those who help the helpers"; see, e.g. Mark A. Lemley* & R. Anthony Reese "Reducing Digital Copyright Infringement Without Restricting Innovation" 56 Stan. L. Rev. 1345, 1345-54, 1373-1426 (2004); Benjamin H. Glatstein "Tertiary Copyright Liability" *The University of Chicago Law Review*, Vol. 71, No. 4 (Autumn, 2004), pp. 1605-1635, as well as Eric Goldman "Offering P2P File-Sharing Software for Downloading May Be Copyright Inducement–David v. CBS Interactive" http://blog.ericgoldman.org/archives/2012/07/inducement_as_a.htm (discussing how courts may view P2P filesharing as a special case) but this theory of liability has typically been dismissed as representing too diffuse a chain of causality, and unsupported by case law.

[58] See, e.g., Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005), 930 (2005).: "[T]hese doctrines of secondary liability emerged from common law principles and are well established in the law." (quoting Blackmun's dissent in *Sony*).

[59] "[T]he lines between direct infringement, contributory infringement, and vicarious liability are not clearly drawn" Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 435(1984).

[60] Pamela Samuelson has hypothesized that the "active inducement" theory laid out in the ***MGM Studios, Inc. v. Grokster, Ltd.***, 545 U.S. 913 (2005), case may amount to a new form of secondary liability. See Pamela Samuelson, *Three Reactions to MGM v. Grokster*, 13 Mich. Telecomm. Tech. L. Rev. (2006).

i. Contributory Infringement

For an OI to be liable for "contributory infringement," the OI must have actual or constructive knowledge of the direct infringement[61] and make a "material contribution" to the direct infringement as well.[62] As can easily be imagined, cases on this turn on the nature of "knowledge" and what sort of contribution is "material". For example, in *Perfect 10 v. Visa International*,[63] the majority found that the role of credit card companies in processing payment transactions for infringing material was too attenuated from the infringing activity to be considered a "material contribution."[64] With respect to knowledge, ignorance of the direct infringement does not necessarily immunize an OI to a claim of secondary liability, since courts have also introduced the idea of "willful blindness"[65] for situations in which a defendant "should have" known about the direct infringement, but deliberately chose not to know about it, or at least chose to not take notice of or act upon facts or circumstances that pointed into the direction of infringement.

Important cases addressing contributory infringement, especially with respect to online intermediaries, are *Sony Corp. of America v. Universal City Studios, Inc*., *Metro–Goldwyn–Mayer Studios Inc. v. Grokster, Ltd*., and the recently settled *Viacom International, Inc. v. YouTube, Inc*.[66] Critically for OIs whose business model or technology may involve copyright infringement, but may also be used in non-infringing ways, the *Sony* case gave rise to the "substantial non-infringing uses" test, borrowed from patent law's "staple article" doctrine, with respect to intermediary technologies that only make direct infringement possible rather than definite. [67]

The court in *Sony* held that in the case of an infringer selling a technology that makes infringement possible, (here, through copying) if a substantial non-infringing use for the technology exists, then the vendor of the technology cannot be found liable[68] because constructive knowledge of the (potential) direct infringement cannot and should not be imputed to the OI. However, the *Grokster* case expanded on and modified this theory, holding that simply because an OI's technology was merely *capable* of substantial non-infringing uses did not categorically immunize the OI from liability, and that contributory liability may still be found if there is clear evidence of an OI's intent to induce and facilitate infringement.[69] This has become known as the *Grokster* "inducement rule."[70]

---

[61] Compare the DMCA's "actual knowledge" requirement 17 USC 512(c)(1)(A)(i)

[62] The classic case on this topic is *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996), although this does not have to do with OIs. The lodestar case for OIs is now *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005), which also adopted the doctrine of "inducement" for copyright liability.

[63] 494 F.3d 788 (9th Cir. 2007)

[64] "Copyright: Infringement Issues - Internet Law Treatise," accessed June 18, 2014, https://ilt.eff.org/index.php/Copyright:_Infringement_Issues.

[65] *In re Aimster Copyright Litigation* 334 F.3d 643, 650 (C.A.7 (Ill.),2003) ("Willful blindness is knowledge, in copyright law (where indeed it may be enough that the defendant *should* have known of the direct infringement")

[66] See: http://www.nytimes.com/2014/03/19/business/media/viacom-and-youtube-settle-lawsuit-over-copyright.html

[67] *Sony Corp. of America v. Universal City Studios, Inc*. 464 U.S. 417, 442 (1984)

[68] "The so-called "Sony safe harbor". See ("the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses.")

[69] *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd*., 545 U.S. 913, 934-935 (2005) ("Thus, where evidence goes beyond a product's characteristics or the knowledge that it may be put to infringing uses, and shows statements or

ii. Vicarious Infringement

For an OI to be liable for vicarious infringement, it must benefit financially from the direct infringement and have both the right and ability to supervise the direct infringer,[71] a concept rooted in the "respondeat superior" doctrine of agency law. Critically for OIs, especially those that are so large that they cannot monitor all the content that they host or is under their purview, actual knowledge of the infringing conduct is not a requirement.[72] It is the OI's ability to supervise the direct infringer that becomes dispositive.

Whether or not an OI has benefitted financially from another's direct infringement may seem like a clear dichotomy. There must be a "causal relationship between the infringing activity and any financial benefit [the] defendant reaps."[73] However, this question has become quite nuanced with respect to the many disparate revenue streams that attach to an OI. As just one example, if an OI hosts third party content, and typically serves advertisements next to that content, for which the OI receives payments, and the content in question proves to infringe copyright, the revenue from that advertising may well be enough to render the OI liable,[74] whether those advertisements appear automatically or are curated.

Whether an OI has the ability to supervise the direct infringer is a fact-specific question, focusing on the relationship between the direct infringer and the would-be secondary infringer. Key cases here are *Fonovisa v Cherry Auction,*[75] where a flea market was held liable for a vendor's infringing sales and *A&M Records, Inc. v. Napster, Inc.*[76] So far, most definitions of "supervision" have been imported from non-Internet fact patterns[77], and no online-specific variation of what it means to be able to "supervise" that might be uniquely applicable to OIs has emerged from the case law. Note, though, that the U.S. Supreme Court in *Grokster* described an

---

actions directed to promoting infringement, *Sony's* staple-article rule will not preclude liability."); See also *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020 (9th Cir. 2013)

[70] *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd*., 545 U.S. 913, 936-937 (2005) ("[O]ne who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.")

[71] Compare 47 U.S.C §230(f)(3)'s "responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." as well as 47 U.S.C §230(f)(4); See *Grokster,* 545 U.S. at 930, for a variant of the definition. ("One ... infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it.")

[72] 3 Nimmer § 12.04[A][1].

[73] "It may also be established by evidence showing that users are attracted to a defendant's product because it enables infringement, and that use of the product for infringement financially benefits the defendant. "Arista Records LLC v. Lime Grp. LLC, 784 F. Supp. 2d 398, 435 (S.D.N.Y. 2011)

[74] *Columbia Pictures Indus. v. Gary Fung*, 710 F.3d 1020 ("Under these circumstances, we hold the connection between the infringing activity and Fung's income stream derived from advertising is sufficiently direct to meet the direct "financial benefit" prong of § 512(c)(1)(B).). but see Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 730 C.A.9 (Cal.), (2007) (Google's ability to terminate an AdSense partnership did not amount to a right or ability to control an infringing AdSense participant.)

[75] *Fonovisa v. Cherry Auction*, 76 F. 3d 259 (9th Cir. 1996).

[76] "*Fonovisa* essentially viewed "supervision" in this context in terms of the swap meet operator's ability to control the activities of the vendors, 76 F.3d at 262, and *Napster* essentially viewed it in terms of Napster's ability to police activities of its users, 239 F.3d at 1023." *Perfect 10, Inc. v. Visa Intern. Service Ass'n* 494 F.3d 788, 802 (C.A.9 (Cal.),2007)

[77] *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd*. 380 F.3d 1154, 1164 -1165 (C.A.9 (Cal.), 2004) ("A salient characteristic of that relationship often, though not always, is a formal licensing agreement between the defendant and the direct infringer") (internal cites omitted)

OI's failure to deploy "filtering tools or other mechanisms to diminish the infringing activity using their software" as giving added significance to other evidence of unlawful objectives and "underscore[ing] Grokster's and StreamCast's intentional facilitation of their users' infringement."[78]

A final note on one of the most basic features of the modern Internet: linking.[79] Whether an OI, such as a search engine, link aggregator, or some other variety of OI can be held secondarily liable for merely linking to directly infringing material is typically described as "unsettled" law.[80] Certainly rights holders, especially large institutional ones, would like to be able to sue wealthy OIs rather than individuals for damages, and OIs who link to content would prefer to be shielded from liability if that content turns out to infringe, but courts have described both a "general principle that linking does not amount to copying," and stated that "Although hyper-linking per se does not constitute direct copyright infringement because there is no copying, in some instances there may be a tenable claim of contributory infringement or vicarious liability."[81] The Supreme Court has also, in a longer discussion of "inducement," unfavorably mentioned providing links to known infringing content.[82] Compare the 2014 European Court of Justice ruling that linking to publicly available material is not infringement, but that linking to restricted or unauthorized material may well be.[83]

2. The DMCA's Safe Harbor

Section 512(c) of the Digital Millennium Copyright Act, "Limitations on liability relating to material online," provides for four separate sets of circumstances in which a "service provider"[84] "shall not be liable for monetary relief." This shield from liability has come to be known as the DMCA's "safe harbor", and these four circumstances are: transitory digital communications, system caching, information residing on systems or networks at direction of users, and

---

[78] *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.,* 545 U.S. 913, 939, 125 S. Ct. 2764, 2781, 162 L. Ed. 2d 781 (2005)

[79] C.f. 17 U.S.C. 512(d)'s "information location tools"

[80] "Copyright: Infringement Issues - Internet Law Treatise."

[81] *Online Policy Grp. v. Diebold,* Inc., 337 F. Supp. 2d 1195, 1202 n.12 (N.D. Cal. 2004) (referencing as notable the DMCA's 512(d).)

[82] *Columbia Pictures Indus., Inc. v. Fung*, 710 F.3d 1020, 1036-1038 (9th Cir. 2013) cert. dismissed, 134 S. Ct. 624, 187 L. Ed. 2d 398 (U.S. 2013)

[83] http://curia.europa.eu/juris/document/document.jsf?text=&docid=147847&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=7778 ("On the other hand, where a clickable link makes it possible for users of the site on which that link appears to circumvent restrictions put in place by the site on which the protected work appears in order to restrict public access to that work to the latter site's subscribers only, and the link accordingly constitutes an intervention without which those users would not be able to access the works transmitted, all those users must be deemed to be a new public, which was not taken into account by the copyright holders when they authorised the initial communication, and accordingly the holders' authorisation is required for such a communication to the public. This is the case, in particular, where the work is no longer available to the public on the site on which it was initially communicated or where it is henceforth available on that site only to a restricted public, while being accessible on another Internet site without the copyright holders' authorisation.").

[84] 17 U.S.C. 512(k) ("(1) Service provider. — (A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.
(B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A)."

information location tools. Of these, the latter two are most germane to a discussion of online intermediaries. It is the "user" explicitly referenced in the "direction of users" that renders the service provider an intermediary, and "information location tools" involve a provider "referring or linking users to an online location".

In each case, the protection from liability that an OI can enjoy is predicated on meeting certain conditions. To enjoy 512(c) immunity regarding infringing "information residing on an OI's system or network at the direction of a user", it must be true that the OI:

- (A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
- (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
- (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to the material;
- (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
- (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

Note the inclusion of the phrases that are similar to the requirements in the two forms of secondary liability. To summarize, an OI is not liable for monetary damages or for injunctive relief, except for the specific types of the latter outlined in 512(j), or for any (allegedly) infringing material on their systems or networks unless they know or have been told it is there and have failed to remove it. It is important to note that if the material in question is not removed, that does not render the OI liable, it simply means they *could be* found liable, whereas if the material in question is removed, there can be no liability regardless of the outcome of a suit against the user.

The language describing the conditions for Section 512(d)'s safe harbor are virtually identical to those in 512(c), in fact using identical language to that of 512(c) regarding notifications, simply clarifying the new variety of information to which the notification refers.[85] It is a DMCA notice submitted under 512(d) that leads to results being removed from Google Search.

There are a also few further requirements described in 512(i) that apply to all of Section 512's safe harbors. An OI should have a "repeat infringer policy" that aims to terminate users of the service that repeatedly infringe and an OI should also accommodate and not interfere with

[85] 512(d)(3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link."

"standard technical measures." In short, an online intermediary can enjoy the Section 512(c) and (d) "safe harbor" and avoid all liability for any copyright infringement committed by its users as long as it expeditiously removes allegedly infringing material once notified of that material's presence, and fulfills Section 512's requirements that apply to all safe harbors. However, the OI may still be subject to the injunctions described in 512(j).

The system's general weighting is therefore toward easy and unquestioned removal. Section 512(f)'s penalties for a sender's misrepresentation in a notice apply only when the misrepresentation is material and knowing, and even then, the only available penalties are attorneys' fees.[86] Section 512(g) absolves the OI from any liability for mistakenly removing material as long as it was done in good faith; under 512(g)(3) a counter-notice sender must swear on penalty of perjury that the material was removed in error; and even in the event of a counter-notice, restoring material that has been removed can happen only after a 10 day period.

C. Other Intellectual Property Laws

1. Trademark

Trademarks are words, phrases, symbols, and other indicia used to identify the source or sponsorship of goods or services. The law allows trademark owners to prevent commercial uses by others that would likely cause customer confusion. Trademark law is recognized at the federal level in the Lanham Act, and every state has an analogous trademark or "unfair competition" law.[87]. To establish ownership of a mark, an aspiring trademark owner must use their trademark in commerce in connection with goods or services.[88]

After ownership is established, the Lanham Act authorizes an owner to bring lawsuits to prevent others from using the mark in a manner that would confuse consumers, or, with respect to more famous marks, to "dilute" mark's distinctiveness across all goods and services.[89] Defenses to a claim of trademark infringement or dilution include that the defendant was selling the plaintiff's genuine goods,[90] that the defendant was using the words that make up the plaintiff's trade name for their normal meaning,[91] and that the defendant was using the plaintiff's mark to refer to the plaintiff directly.[92]

---

[86] The standard for misrepresentation is quite high as it requires "actual knowledge" of misrepresentation on the part of the copyright owner: Rossi v. Motion Picture Association of America, Inc., 391 F.3d 1000 (9th Cir. 2004), 1005 (2004).: "A copyright owner cannot be liable simply because an unknowing mistake is made, even if the copyright owner acted unreasonably in making the mistake.""

[87] *See State Trademark Information and Links*, U.S.P.T.O., http://www.uspto.gov/trademarks/process/State_Trademark_Links.jsp (last updated July 24, 2012).

[88] *See* RESTATEMENT (THIRD) UNFAIR COMPETITION § 18.

[89] *See What Trademark Covers*, DIGITAL MEDIA LAW PROJECT, http://www.dmlp.org/legal-guide/what-trademark-covers (last updated April 30, 2008). A trademark owner can also bring a claim of dilution by "tarnishment," or the use of a trade name that harms the reputation of a famous mark. 15 U.S.C. § 1125(c)(2)(C).

[90] *See, e.g.*, Prestonettes, Inc. v. Coty, 264 U.S. 359 (1924).

[91] This is sometimes called a "descriptive fair use." *See, e.g.*, KP Permanent Make-Up, Inc. v. Lasting Impression I, Inc., 543 U.S. 111 (2004).

[92] This is called a "nominative fair use, and tends to also include the requirement that the mark at issue must not be readily identifiable without use of the mark's name, the use of the mark must be limited to as much as is necessary to identify the mark, and the user must do nothing that would suggest sponsorship or endorsement by the trademark owner. The New Kids on the Block v. News America Publ'g, Inc., 971 F.2d 302 (9th Cir. 1992). Critics note that

Trademark law is unique in this study, as there is no equivalent to general content liability's Section 230 or copyright's Section 512 "safe harbor" to address online intermediary liabilities. Section 230 of the Communications Decency Act does not protect online intermediaries from trademark liability under the Lanham Act,[93] and courts are split as to whether it protects against claims under state trademark laws.[94] As a result, much of recent trademark law reflects a judicial attempt to reinterpret existing tests in light of online activity, which has led to less legal certainty. Because trademark draws from both state and federal laws, precedent in this area is especially complex.

Existing Supreme Court precedent recognized secondary trademark liability for those who intentionally induce another to infringe a trademark, as well as those who manufacture or distribute supplies to another, knowing that person is engaging in trademark infringement.[95] Lower courts have extended that to cases where the defendant supplies a platform for the sale of trademark-infringing goods, such as the operator of a flea market, when a plaintiff can show that platform operator knew about infringing activity. These courts, however, have not imposed an affirmative duty to take precautions against counterfeits.[96]

Applying these principles to the online context, courts generally agree that online intermediaries can be held liable for infringement, but establishing clear standards for that liability has been more divisive.[97] In one early case, a court stated that an Internet company could be liable under a theory of contributory trademark infringement if it possessed "direct control and monitoring" over the infringing activity of third parties on the site, though it declined to extend that theory to the defendant, a domain name resolution service.[98] In a prominent 2010 case, *Tiffany* v. *eBay* (discussed in the "Private Ordering to Respond to Trademark Concerns – eBay's VERO Program" case study below) a federal appellate court upheld the infringement-management practices of the online auction website eBay, who took down infringements upon receipt of specific rights holder complaints.[99] Critically, the court held that general knowledge that the defendant's platform was being used for infringing activity on the platform was not sufficient; plaintiffs would have to show that a defendant has knowledge of specific infringing conduct.[100]

For online auction sites, the holding in *Tiffany* likely means increased industry homogeneity as competitors attempt to craft their own business as in the mold of eBay's judicially accepted

---

this is, in effect, the same test as the general likelihood of confusion test. *See* William McGeveran, *Rethinking Trademark Fair Use*, 94 IOWA L. REV. 49, 90-97 (2008).

[93] *See, e.g.*, Parker v. Google, Inc. 442 F. Supp. 2d 492, 502 n.8 (E.D. Pa. 2006).

[94] *Compare* Perfect 10, Inc. v. CCBill, LLC 488 F.3d 1102, 1118-19 (9th Cir. 2007) (Section 230's exception for "intellectual property" only covers federal intellectual property laws); *with* Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288, 298-302 (D.N.H. 2008) (extensively analyzing *Perfect 10* and deciding that Section 230 does extend to state intellectual property laws).

[95] Inwood Labs., Inc. v. Ives Labs., Inc., 456 U.S. 844, 853-54 (1982).

[96] Hard Rock Cafe Licensing Corp. v. Concession Services, Inc., 955 F.2d 1143, 1149 (7th Cir. 1992); Fonovisa Inc. v. Cherry Auction Inc., 76 F.3d 259, 265 (9th Cir. 1996).

[97] *See e.g.*, Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 984 (9th Cir. 1999); Rescuecom Corp. v. Google Inc., 562 F.3d 123 (2d Cir. 2009); Playboy Ent., Inc. v. Netscape Comm'ns Corp., 354 F.3d 1020, 1024 (9th Cir. 2004); Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93 (2d Cir. 2010); Rosetta Stone Ltd. v. Google, Inc., 676 F.3d 144, 149 (4th Cir. 2012).

[98] Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 984 (9th Cir. 1999).

[99] Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93 (2d Cir. 2010).

[100] *Id.* at 107.

model. For other online intermediaries, the lack of a legal standard means increased risk and wary innovation. For an enterprising online intermediary with a service susceptible to a claim of contributory trademark infringement, looking to the policies and standards underlying the CDA and DMCA are likely the best barometers of legal guidance.[101]

2. Misappropriation and Right of Publicity Laws

Two overlapping types of laws govern the use of a person's name or likeness for commercial or exploitative purposes without the person's consent: right of publicity laws and laws against misappropriation of a person's name or likeness.[102] While the two types of laws cover the same conduct, they are meant to remedy different harms: misappropriation is meant to remedy the damage to human dignity for unauthorized commercialization, while right of publicity is meant to compensate for commercial damage for lost licensing revenue.[103] Like the privacy torts discussed above, knowing participation in another's violation could lead to intermediary liability, though there are very few cases on point.[104]

Courts unanimously agree that federal intellectual property claims are not covered by the CDA, but there is ongoing disagreement over whether the exception also extends to state intellectual property claims, particularly claims involving states' right of publicity laws.[105] Other courts have taken the middle path, noting the difficulty of the issue and refusing to consider whether state intellectual property rights are exempted by the CDA when other means of settling the claim exist.[106] This echoes a concern articulated in the discussion of CDA 230 above: while Section 230 by its terms provides a clear and direct means for foreclosing intermediary liability, courts have allowed extensive and costly litigation on the question, undercutting its positive effects for intermediaries.[107]

---

[101] At present, the most considerable legal attention to intermediaries has come not for actions they take with respect to user content, but to their own direct liability. This is in contrast to earlier times, where direct liability was rarely found with online service providers. Emily Favre, *Online Auction Houses: How Trademark Owners Protect Brand Integrity Against Counterfeiting*, 15 J.L. & POL'Y 165, 179 (2007). Two recent federal appellate cases have taken issue with Google's AdWords program, which allows companies to buy advertisement to display alongside searches for certain words, including the names of competing companies. *See* Rescuecom Corp. v. Google, Inc., 562 F.3d 123 (2d Cir. 2009); *Rosetta Stone Ltd. v. Google, Inc.*, 676 F.3d 144, 149 (4th Cir. 2012). Both cases subsequently settled.

[102] *See generally Using The Name or Likeness of Another*, DIGITAL MEDIA LAW PROJECT, http://www.dmlp.org/legal-guide/using-name-or-likeness-another (last updated July 30, 2008).

[103] J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 28:6 (4th ed. 2014).

[104] Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1183 (C.D. Cal. 2002) (finding a likelihood of success on an claim for aiding another's right of publicity violation); *but see* Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 809 (9th Cir. 2007) (declining to find authority for a credit card processor for aiding and abetting a right of publicity violation, "[e]ven if such liability is possible under California law – a proposition for which [plaintiff] has provided no clear authority"); Keller v. Electronic Arts, Inc., No. 09-cv-1967, 2010 WL 530108 at *2 (N.D. Cal. 2010) *aff'd on other grounds sub nom.* In re NCAA Student-Athlete Name & Likeness Licensing Litigation, 724 F.3d 1268 (9th Cir. 2013) (finding no theory of liability for those who enable another's right of publicity violation).

[105] *Compare* Perfect 10, Inc. v. CCBill, LLC 488 F.3d 1102, 1118-19 (9th Cir. 2007) (Section 230's exception for "intellectual property" only covers federal intellectual property laws); *with* Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288, 298-302 (D.N.H. 2008) (extensively analyzing *Perfect 10* and deciding that Section 230 does extend to state intellectual property laws).

[106] Almeida v. Amazon.com, Inc., 456 F.3d 1316 (11th Cir. 2006).

[107] *See generally* Ardia, *supra* note [[x]].

3. The Espionage Act

Because of the considerable attention given toward the dissemination of classified government information through the documents released by Chelsea Manning and Edward Snowden, and the profound policy implications of both the information they conveyed and the treatment of those who handle and disseminate such documents to the public, special attention should be given to a particular federal crime that implicates the disclosure of classified information. The Espionage Act of 1917 contains many provisions intended to prohibit interference with military operations and protect national security.[108] These include provisions that criminalize obtaining, collecting, or communicating information that would harm the harm the national defense of the United States.[109] This section was used by the United States government to go after the New York Times and Washington Post for their publication of "The Pentagon Papers," a classified and damning assessment of United States involvement in the Vietnam War.[110] Most recently, it was used to convict former U.S. Army intelligence analyst Chelsea Manning for leaking classified documents to the organization WikiLeaks.[111]

While all federal criminal law includes the possibility for a charge of aiding and abetting another's violation of the law,[112] the United States has never successfully prosecuted an information intermediary for disseminating classified information under the Espionage Act.[113] Such a theory would present profound First Amendment issues, and ultimately an intermediary may only be found liable if the intermediary bribed, coerced, or defrauded a government employee to disclose classified information.[114]

4. Surveillance Law

A patchwork of federal law enables both law enforcement and intelligence agencies to compel online intermediaries (as well as others) to disclose data about their users, sometimes including the content of their communications. The federal requirements for the disclosure of user data are mainly found in two places. The primary authority enabling the federal government to compel companies to surrender customer data in criminal investigations is found in the Stored Communications Act (SCA). The authority for intelligence investigations is found primarily in the Foreign Intelligence and Surveillance Act (FISA) and related amendments to the SCA. The authority used to compel the data disclosure is important for several reasons: it determines the

---

[108] *See* 18 U.S.C. §§ 793–798.
[109] 18 U.S.C. § 793(e).
[110] New York Times Co. v. United States, 403 U.S. 713 (1971).
[111] Cora Currier, *Charting Obama's Crackdown on National Security* Leaks, PRO PUBLICA, July 30, 2013, http://www.propublica.org/special/sealing-loose-lips-charting-obamas-crackdown-on-national-security-leaks. Many others have been charged but not ultimately convicted for violating the Espionage Act or conspiracy to violate the Espionage Act.
[112] 18 U.S.C. § 2; *see also* § 793(g) ("If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.").
[113] *See* Emily Peterson, *WikiLeaks and the Espionage Act of 1917: Can Congress Make It a Crime for Journalists to Publish Classified Information?*, THE NEW MEDIA AND THE LAW VOL. 35 NO. 3, Summer 2011, *available at* http://www.rcfp.org/browse-media-law-resources/news-media-law/wikileaks-and-espionage-act-1917.
[114] *See* Geoffrey R. Stone, *Government Secrecy vs. Freedom of the Press*, 1 HARV. L. & POL'Y REV. 185, 217. For more on the general First Amendment right to disclose true matters of public concern, *see supra* notes 21, 26 and accompanying text.

legal standard that must be used, the kind of data that can be collected, and even how companies can write their transparency reports.

The SCA is an outdated law, enacted well before high-speed Internet or gigabytes of free cloud storage was the norm. The SCA gives law enforcement agencies the ability to collect substantial personal data, often with minimal court supervision. Under the framework of the SCA, there are three primary methods for compelling data collection: warrants, court orders, and subpoenas.

The easiest form of legal process to obtain is a subpoena. Instead of going before a court or a judge, a law enforcement agent can directly issue a subpoena to a company if there is any reasonable possibility that the materials will produce information relevant to the general subject of the investigation. Because it is so easy to obtain a subpoena, the types of information that law enforcement can obtain subject to a subpoena are fairly circumscribed. Using a subpoena, law enforcement can obtain what is known as "basic subscriber information." This includes the user's name, address, connection records (including session times and durations), the date the user began using services, the types of services used, the IP address or other instrument number, and payment information (including credit card and bank account numbers).

The next type of legal process, slightly more difficult to obtain, is a 2703(d) order, called that because it is described in section 2703(d) of the SCA. A "d order" is a court order, meaning that unlike a subpoena it requires a law enforcement agent to go before a court and show that there are "specific and articulable facts showing that there are reasonable grounds to believe" that the requested data is "relevant and material to an on-going criminal investigation."[115] The d order allows law enforcement to collect non-content information, which includes data such as e-mail headers, recipient e-mail addresses, and any other account logs that the provider may maintain.

As described above, both subpoenas and d orders can be used to get data other than content. However, the data that law enforcement is most likely to be interested in would be classified as "content," and includes things such as e-mail subject lines, e-mail content, and instant message text. Under the letter of the law, both subpoenas and d orders may be used in certain limited circumstances to also get content information. For instance, the law allows law enforcement to obtain opened e-mails or other stored files, or unopened e-mail in storage for more than 180 days, using just a subpoena or a d order, as long as law enforcement provides notice to the user.[116]

Although the text of the law enables law enforcement to obtain content information, in limited circumstances, with only a d order or a subpoena, in actuality, law enforcement generally needs to use a third type of process to get content information: a warrant. Despite the text of the SCA, the U.S. Court of Appeals for the 6th Circuit, with jurisdiction over the states of Ohio, Michigan, Kentucky, and Tennessee, held in *United States v. Warshak* that the government needs a warrant to obtain e-mail content.[117] Although that holding is technically limited to the geographic region of the 6th Circuit, almost all the major Internet companies rely upon the *Warshak* decision to

[115] 18 U.S.C. § 2703(d).
[116] *See* 18 U.S.C. § 2703(a), (b).
[117] *See* 631 F.3d 266 (6th Cir. 2010).

require a warrant before providing any content information, despite the fact that such a conclusion is seemingly inconsistent with the SCA itself.[118]

Because a search warrant allows for the collection of content, and is therefore more invasive than subpoenas and d orders, it is also harder to obtain. To obtain a warrant, a law enforcement agent must demonstrate to a court that there is "probable cause" that information related to a crime is in the specific place to be searched. In addition to content information, warrants can obtain all the non-content data that a d order and subpoena can collect (and a d order can collect all the subscriber information that a subpoena can collect).

For terrorism or national security related investigations, the government has three additional levers for the collection of data from online intermediaries. National Security Letters (NSLs) allow the FBI to obtain telephone and e-mail records (and associated billing records), "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities," but not the content of the messages themselves.[119] Section 215 of the USA PATRIOT Act amended FISA to enable secret court orders, approved by the Foreign Intelligence Surveillance Court (FISC), to require third parties, such as ISPs or telephone providers, to provide business records deemed relevant to terrorism or intelligence investigations. The government used the Section 215 authority, for example, to compel Verizon to provide all cell phone metadata.[120] The third lever is Section 702 of the FISA Amendments Act, which allows the government to collect both the content and non-content information of targeted non-U.S. persons reasonably believed to be outside of the United States.

Subpoenas, d orders, warrants, 215, and 702 orders represent just some of the wide array of legal tools at the disposal of American law enforcement and intelligence agencies. Additional tools include wiretaps and pen-registers, which enable law enforcement to obtain prospective, instead of retrospective, data. With this array of tools and the treasure trove of personal information that online intermediaries may store, it means that once intermediaries reach a sufficiently large size, it is only a matter of time before law enforcement or intelligence agencies will serve legal process.

[118] *See, e.g.*, *Twitter Transparency Report* at https://transparency.twitter.com/country/us (" A properly executed warrant is required for the disclosure of the contents of communications (e.g., Tweets, DMs).").
[119] 18 U.S.C. § 2709(b)(2).
[120] Full text of Section 215 Order the government served on Verizon.
http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order

III. Case Studies

A. Sex Trafficking in Online Classified Advertising – Craigslist.org and Backpage.com

1. Introduction

As discussed in the Legal Landscape Primer of this report, Section 230 of the Communications Decency Act enables a wide array of online intermediaries to operate within the United States without the burdens of either monitoring user-generated content or (except in the case of certain intellectual property claims) implementing a system for removal for such content.

While this has facilitated the creation of many platforms for user-generated content, Section 230's protections are controversial. Many believe that the rule protects what is worst about the Internet and social media rather than what is best about it. Plaintiffs who legitimately claim to be harmed, as well as law enforcement officials attempting to protect the public, are often frustrated by their inability to stem unlawful online content at the obvious source, the intermediary. This frustration is particularly acute when the websites that provide access to such content seem to revel in (and profit from) their users posting content that is tawdry or mean-spirited, or even illegal under state laws.

This case study examines a six-year effort by officials of state (rather than federal) government to hold intermediaries accountable for a specific activity: namely, the hosting of online advertisements alleged to facilitate prostitution and sex trafficking. A recurring theme throughout this case study is the barrier that Section 230 poses to efforts by state governments to shut down these advertisements, and the ways that these governments have attempted to circumvent Section 230 through public pressure, judicial action, and legislation.

This case study focuses on two websites in particular, Craigslist and Backpage.com:

- **Craigslist** is a classified advertisements service that has been available via the Internet since 1996, and currently the largest such online service in the United States. Craigslist hosts separate sub-domains for separate geographic regions; more than 700 regions in seventy countries currently have Craigslist sites, with content available in multiple languages. Listings on the site include advertisements and solicitations for jobs, housing, the sale of personal items, and various services. The listings for services originally included a section for "erotic services." Craigslist's terms of service expressly prohibit the use of the site to advertise illegal activities.

- **Backpage.com**, launched in 2004, is the second largest online classified advertisements service in the United States after Craigslist. Like Craigslist, it offers listings for a wide range of proposed transactions and is available in multiple countries and languages. Backpage.com was originally owned by Village Voice Media. The site contains a section for "adult entertainment services," but, like Craigslist, prohibits the use of the site to advertise illegal activities.

2. "Erotic" and "Adult" Advertisements on Craigslist – Negotiation Leads to Concession

As a general classified advertising service, Craigslist had hosted a section of "erotic services" content on its service, created by its users and over which Craigslist could plausibly claim immunity for intermediary liability under Section 230. While Craigslist's protection under Section 230 was never pierced and adult content had been on the site for years, a series of events taking place from March 2008 to September 2010 lead to the rapid shutdown of these listings on the site.

The "erotic services" section on Craigslist attracted the attention of state and local law enforcement in the United States, after it was perceived that some users were using the section to advertise services that were illegal under state law. In March 2008, the attorney general of Connecticut, Richard Blumenthal, sent a letter to Craigslist on behalf of the attorneys general of 40 states, demanding that Craigslist purge the site of ads for prostitution and illegal sex-oriented businesses and more effectively enforce its own terms of service, which prohibit illegal activity.[121]

Craigslist first opted to respond to these demands through negotiation. In November 2008, Craigslist reached an agreement with these state attorneys general to take steps to curb – but not remove – its "erotic services" listings. These steps included requiring posters to provide valid telephone numbers and pay a small fee per ad using a credit card, in order to make posters easier for law enforcement to track.[122] Jim Buckmaster, chief executive of Craigslist, stated that the attorneys general had "identified ads that were crossing the line," and that the company "saw their point, and . . . resolved to see what [it] could do to get that stuff off the site."[123] Craigslist subsequently reported a 90% drop in erotic services listings.[124]

Four months later, a sheriff for the county in Illinois that includes Chicago, Thomas Dart, sued Craigslist in federal court. Dart claimed that the site created a "public nuisance" under Illinois law, because its "conduct in creating erotic services, developing twenty-one categories, and providing a word search function causes a significant interference with the public's health, safety, peace, and welfare."[125] Craigslist moved for judgment on the pleadings in the case on the basis of Section 230, asserting that Dart was attempting to hold Craigslist liable as the "publisher or speaker" of content created by third party users.[126] Craigslist would ultimately win that case on Section 230 grounds in October 2009.[127]

While that litigation was pending, in April 2009, Philip Markoff (later dubbed the "Craigslist killer") murdered one woman whose services he located through Craigslist and robbed two others; the case received national attention.[128] The following month, the attorney generals of

---

[121] http://blog.sfgate.com/techchron/2008/03/27/craigslist-gets-heat-for-prostitution-ads/
[122] http://www.dmlp.org/sites/citmedialaw.org/files/2008-11-00-Craigslist%20AG%20Agreement.pdf
[123] http://www.nytimes.com/2008/11/07/technology/internet/07craigslist.html
[124] http://arstechnica.com/tech-policy/2009/03/craigslist-over-90-drop-in-erotic-services-over-last-year/
[125] http://www.dmlp.org/sites/citmedialaw.org/files/2009-03-05-Dart%20Complaint.PDF
[126] http://www.dmlp.org/sites/citmedialaw.org/files/2009-05-04-Memo%20in%20Support%20of%20Craigslist%27s%20Motion%20for%20Judgment%20on%20the%20Pleadings.pdf
[127] *Dart v. Craigslist, Inc.*, 665 F. Supp.2d 961 (N.D. Ill. 2009). Dart did not appeal the decision.
[128] http://www.cbsnews.com/news/the-craigslist-killing-case-overview/

Illinois, Connecticut, and Missouri met with Craigslist executives again, seeking an end to ads alleged to be advertisements for illegal sexual activities.[129] That same month the attorney general of South Carolina, Henry McMaster, sent Craigslist a letter accusing it of violating its November 2008 agreement and threatening the company's management with criminal investigation and prosecution; the letter stated that "[i]t appears that the management of craigslist has knowingly allowed the site to be used for illegal and unlawful activity after warnings from law enforcement officials and after an agreement with forty state attorneys general."[130]

While never found civilly or criminally liable, Craigslist subsequently removed its "erotic services" section and replaced it with an "adult services" section, in which employees would take an active role in reviewing postings for indications of activity that was illegal or otherwise violated the site's guidelines.[131] Jim Buckmaster, CEO of Craigslist, denied that this change was the result of legal pressure, instead stating that the change was "strictly voluntary," that the site's activities were always protected by Section 230, and that "[i]n striking this new balance we have sought to incorporate important feedback from all the groups that have expressed strongly held views on this subject, including some of the state A.G.'s, free speech advocates and legal businesses who are accustomed to being entitled to advertise."[132] New York Attorney General Andrew M. Cuomo criticized the move, stating that rather than work with his office "to prevent further abuses, in the middle of the night, Craigslist took unilateral action which we suspect will prove to be half-baked."[133]

At the same time, in an attempt to forestall the threat from the South Carolina Attorney General, Craigslist filed a declaratory judgment action against McMaster in federal district court in South Carolina, asserting that McMaster's threats violated the First Amendment by chilling Craigslist's speech and that the threatened prosecution would be blocked by the First Amendment and Section 230.[134] McMaster consented to a preliminary injunction against prosecution of Craigslist while this lawsuit was pending.[135] The court ultimately dismissed Craigslist's complaint without reaching the Section 230 issue, holding that there was no actual case or controversy ripe for adjudication on that issue because no prosecution had been initiated.[136] In May 2010, approximately one year after Craigslist's "erotic services" section was closed and the new "adult services" section was launched, Connecticut and 38 additional states sent subpoenas to Craigslist asking for information about the site's revenue from sex-related advertisements and its implementation of measures to stop the use of the site for prostitution. This move was believed to have resulted from the widespread perception that Craigslist's "adult services" section had not reduced the use of the site for prostitution, but simply driven it into other sections of the site

[129] http://www.pantagraph.com/business/attorney-general-madigan-craigslist-dropping-erotic-services-ads/article_1c791ce9-2e57-5f18-b223-72fe8a679204.html
[130] http://www.dmlp.org/sites/citmedialaw.org/files/2009-05-05-South%20Carolina%20AG%20Letter.pdf
[131] http://www.nytimes.com/2009/05/14/technology/companies/14craigslist.html
[132] http://www.nytimes.com/2009/05/14/technology/companies/14craigslist.html
[133] http://legalblogwatch.typepad.com/legal_blog_watch/2009/05/ny-ag-appears-miffed-at-craigslist.html
[134] http://www.dmlp.org/sites/citmedialaw.org/files/2009-05-20-Craigslist%20Complaint%20for%20Declaratory%20Relief.pdf
[135] http://www.dmlp.org/sites/citmedialaw.org/files/2009-05-22-Consent%20TRO%20in%20Craigslist%20v.%20McMaster.pdf
[136]http://scholar.google.com/scholar_case?q=craigslist+v+mcmaster&hl=en&as_sdt=40000006&case=14896321323836850885&scilh=0

using coded terminology for the services offered. Craigslist accused Connecticut's attorney general of engaging in blatant political grandstanding. [137]

Public pressure on Craigslist came from a different direction two months later, when two teenage girls published an open letter to Craig Newmark, the founder of Craigslist, stating that they had been the victims of sex trafficking through the site.[138] By August 2010, there were public calls for the "adult services" section to be shut down, both in the press[139] and from state law enforcement.[140] Buckmaster responded to these demands, saying:

> "[f]ortunately, most concerned parties seem to realize that declassifying adult services ads back into Craigslist personals, services, and other categories, and off site to venues that have no interest in combating trafficking and exploitation or in assisting law enforcement, would simply undo all the progress we have made, undermine our primary mission of evolving Craigslist community sites according to user feedback, set back the efforts of our partners in law enforcement and exacerbate the very societal epidemic we all seek to end."[141]

Less than a month later, however, Craigslist shuttered the "adult services" section in the United States. As of September 4, 2010, the link to the section on Craigslist was replaced with a black label reading "censored."[142] This label (and the dead link to the defunct section) was removed a few days later.[143] Craigslist later removed the section from all of its sites worldwide.[144]

Later that month Craigslist representatives appeared at a hearing of the House Judiciary Committee and testified that while the "adult services" section had been removed permanently from the United States, it was unrealistic to believe that this would end sex crimes. By pressuring Craigslist to close the section, they claimed, state governments had ended their ability to contain the illegal activity in one location and work with Craigslist to pursue offenders; now, this traffic would simply migrate to other sites. Craigslist's representatives specifically pointed to a spike in traffic to Backpage.com following the shutdown of Craigslist's section.[145]

3. "Adult Content" on Backpage.com – State Legislation and Defiance

Six days after Craigslist testified, twenty-one state Attorneys General sent a public letter to Backpage.com demanding that it close its "adult entertainment services" section, stating that the "volume of these ads will grow in light of Craigslist's recent decision to eliminate the adult services section of its site. In our view, it is time for the company to follow craigslist's lead and take immediate action to end the misery of the women and children who may be exploited and victimized by these ads."[146]

---

[137] http://arstechnica.com/tech-policy/2010/05/craigslist-brothel-business-under-fire-again/
[138] http://www.cnn.com/2010/OPINION/08/02/saar.craigslist.child.trafficking/index.html
[139] Id.
[140] http://bostonherald.com/news_opinion/local_politics/2010/08/martha_coakley_tells_craigslist_abandon_adult_sex_ads; http://www.cnn.com/2010/CRIME/08/25/craigslist.adult.content/index.html?hpt=Mid
[141] http://www.cnn.com/2010/OPINION/08/04/buckmaster.craigslist.rebuttal/index.html?hpt=C2
[142] http://www.nytimes.com/2010/09/05/technology/05craigs.html?_r=2&hp&
[143] http://www.cnet.com/news/craigslist-removes-censored-bar-from-site/
[144] http://arstechnica.com/tech-policy/2010/12/craigslist-shuts-down-adult-services-worldwide/
[145] http://www.nytimes.com/2010/09/16/business/16craigslist.html?_r=0
[146] http://www.state.ia.us/government/ag/latest_news/releases/sept_2010/Backpage_letter.pdf

Backpage.com publicly rejected the states' demand that same day, writing:

> "Backpage.com respectfully declines the recent demand by a group of 21 state attorneys general that it close its adult classifieds website . . . Backpage.com is a legal business and operates its website in accordance with all applicable laws . . . Censorship will not create public safety nor will it rid the world of exploitation."[147]

Nevertheless, on October 18, 2010, Backpage.com announced that it would temporarily suspend certain aspects of its adult sections while implementing improved screening procedures for advertisements for illegal services.[148]

The next several months saw relatively little government activity or public outcry against Backpage.com itself. There were, however, numerous media reports of arrests for illegal prostitution and human trafficking in various states, which were attributed to law enforcement's identification of offenders via Backpage.com.[149]

Beginning in July 2011, there were renewed demands from both local officials and private actors for Backpage.com to reform or remove its adult services section.[150] That summer, forty-six state attorneys general sent a public letter to Backpage.com calling for information about how the site attempts to remove advertising for sex trafficking, especially ads that could involve minors. The letter pointed to more than fifty cases involving the trafficking or attempted trafficking of minors through Backpage.com.[151] A petition signed by 80,000 people and spearheaded by John Buffalo Mailer, the son of Village Voice co-founder Norman Mailer, later demanded that the Village Voice shut down the adult services section.[152] The Village Voice would subsequently divest itself of Backpage.com, which continued to operate independently.[153]

At the Spring 2012 meeting of the National Association of Attorneys General (NAAG), Washington State Attorney General Rob McKenna gave a speech to attendees in which he made clear that the fundamental problem in dealing with Backpage.com was Section 230:

> "[M]embers of Congress may want to review section 230 of the Communications Decency Act in order to make sure that when Backpage goes away, another operation based on exploitation doesn't fill the void…Backpage executives see the CDA as a license to make money from prostitution ads without any accountability. I disagree with their assessment. The CDA does not immunize Web sites from criminal prosecutions

---

[147] http://www.altweeklies.com/aan/Backpagecom-rejects-calls-for-censorship/Article?oid=2802426

[148] http://www.businesswire.com/news/home/20101018005791/en/Backpage.com-Suspend-Areas-Personals-Adult-Sections-Implements#.U2E1yye0y8E

[149] http://www.civilbeat.com/articles/2010/12/29/7649-unclassified-backpagecom-an-adult-hub/; http://www.seacoastonline.com/apps/pbcs.dll/article?AID=/20110106/NEWS/110109879/-1/NEWSMAP; http://www.washingtoncitypaper.com/blogs/citydesk/2011/03/08/d-c-cops-targeting-backpage-com/; http://www.examiner.com/article/prostitution-has-backpage-com-picked-up-where-craigslist-left-off

[150] See, e.g., http://slog.thestranger.com/slog/archives/2011/10/25/clergy-takes-out-ny-times-ad-pressures-village-voice-to-end-sex-trafficking-in-its-publications; http://www.scribd.com/doc/70170993/Groundswell-letter-to-VVM

[151] http://www.atg.wa.gov/pressrelease.aspx?id=28896#.U0bj1McwIhM

[152] http://www.prnewswire.com/news-releases/village-voice-founders-son-criticizes-company-for-advertisements-that-others-can-use-for-sex-trafficking-of-minors-joins-groundswell-campaign-137170558.html

[153] http://www.csmonitor.com/Business/Latest-News-Wires/2012/0924/Village-Voice-cuts-ties-from-sex-ad-linked-Backpage.com

> under federal law, though the states are currently hampered in their ability to take enforcement action. However, given that sites such as Backpage see this federal statute as an invitation to promote human trafficking without consequence, Congress should hold hearings about carefully revising the law to ensure that the knowing promotion of prostitution, for example, is more easily pursued by state authorities, in addition to their federal counterparts."[154]

That same month, the State of Washington passed Senate Bill 6251, a state law that criminalized commercial advertising for sexual abuse of a minor.[155] The bill made it a felony to knowingly publish, disseminate, or display or to "directly or indirectly" cause content to be published, disseminated or displayed if it contains a depiction of a minor and any "explicit or implicit offer" of sex for something of value. Under the proposed law, it was not a valid defense that the defendant did not know the age of the person depicted.

The State of Tennessee followed suit shortly thereafter by enacting Tennessee Public Charter No. 1075, which criminalized selling advertisements involving commercial sex with anyone appearing to be a minor. As with the Washington law, the seller's ignorance of the fact that a person depicted was a minor was not a defense to criminal liability; the only recognized defense was if the seller individually verified the age of anyone appearing in an advertisement via government-issued identification. To implement such a system on a website would be, in all likelihood, prohibitively expensive.

These statutes were expressly targeted at Backpage.com's advertising, notwithstanding the fact that Section 230 barred the imposition of such liability under state law. In June 2012, Backpage.com filed two separate lawsuits in federal courts in Washington and Tennessee to prevent the enforcement of these laws, arguing that they were preempted by Section 230 and violated the First Amendment by chilling a substantial amount of legal advertising to adults.[156]

The cases were swiftly resolved in Backpage.com's favor. In each case, the court granted a temporary restraining order against enforcement of the law on the basis of Section 230 and the First Amendment.[157] Washington State settled with Backpage.com in December 2012, agreeing to pay $200,000 in attorneys' fees and to work to repeal SB 6251.[158] Meanwhile, the State of Tennessee did not oppose Backpage.com's motion to convert the restraining order to a permanent injunction, ending the Tennessee case in March 2013.[159]

4. Attention Turns to Section 230 Itself – The Current Legislative Debate

The failure of these laws fueled a legislative attack on Section 230. On July 23, 2013, forty-nine state and territory attorneys general sent an open letter to four members of Congress citing the activities of Backpage.com and calling upon Congress to amend Section 230. The letter cited to the Washington and Tennessee cases, among others, as evidence that Section 230 was frustrating

---

[154] http://www.kirk.senate.gov/?p=blog&id=434
[155] http://apps.leg.wa.gov/documents/billdocs/2011-12/Pdf/Bills/Session%20Laws/Senate/6251-S.SL.pdf
[156] http://bigstory.ap.org/article/backpagecom-sues-over-wash-sex-trafficking-law; http://nashvillecitypaper.com/content/city-news/backpagecom-sues-state-halt-law-aimed-online-child-sex-ads
[157] http://www.atg.wa.gov/uploadedFiles/Another/News/Order%20Granting%20Preliminary%20Injunction.pdf; http://www.timesnews.net/article/9055788/judge-tennessee-law-that-targets-online-sex-ads-infringes-on-free-speech
[158] http://www.atg.wa.gov/pressrelease.aspx?id=30787#.U0bIgMcwIhM
[159] http://www.dmlp.org/threats/backpagecom-v-cooper-et-al

attempts by state law enforcement to suppress sex trafficking, and accordingly asked that Congress amend Section 230 to include an exception for state criminal law, as it currently does for federal law.[160]

This proposal was widely criticized by academics and advocates of online freedom, because it would effectively eviscerate Section 230; states could avoid federal preemption simply by criminalizing any conduct by intermediaries of which they disapproved. The Electronic Frontier Foundation noted that the proposed amendment would grant states legislative authority over the Internet that was much broader than the sex trafficking issue that allegedly motivated the proposal, and would be dangerous to freedom of expression online.[161] Professor Eric Goldman of Santa Clara University School of Law called the NAAG's proposal "a terrible idea" and "one of the most serious threats to Section 230's integrity that we've ever faced," arguing that the amendment would subject Internet communication and commerce to the whims of vague, conflicting, and provincial state legislation.[162]

The demand by the state attorneys general has not yet resulted in a movement within the U.S. Congress to amend Section 230; Congress has instead looked to expand federal sex trafficking law to cover advertising. On March 13, 2014, Rep. Ann Wagner introduced H.R. 4225, the "Stop Advertising Victims of Exploitation (SAVE) Act of 2014" in the U.S. House of Representatives.[163] In its final form, H.R. 4225 seeks to amend the current federal law against sex trafficking. As currently enacted, the law punishes (among other things) anyone who "knowingly . . . recruits, entices, harbors, transports, provides, obtains, or maintains by any means a person" knowing or in reckless disregard of the fact that either (1) the person is a minor who will be engaged in a commercial sex act; or (2) the person is of any age, but will be so engaged through means of force, fraud, or coercion. A separate offense exists for someone who benefits financially from these activities, provided they also satisfy the same knowledge requirement.[164]

The bill would add "advertises" to the list of prohibited behavior. It would require those who financially benefit from advertising sex trafficking have actual knowledge of such, but allows those doing the advertising to be liable if the only are "reckless[ly] disregard[ing] the fact" that such person is a victim of sex trafficking. The bill does not clarify whether a platform, like Backpage.com or Craigslist, would be considered as the advertiser or the financial beneficiary. If it is considered the advertiser, this would mean a platform could be liable without first showing specific knowledge of the activity, in stark contrast to most other forms of online intermediary liability. As it would be a federal criminal law, Section 230 would also offer no defense.

Some members of the media and civil liberties organizations have expressed concerns with this legislation. The Association of Alternative Newsmedia published an editorial in April attacking H.R. 4225, raising First Amendment concerns similar to those previously raised by

[160] https://www.eff.org/sites/default/files/cda-ag-letter.pdf The proposed legislative amendment would add the words "or State" to 47 U.S.C. § 230(e)(1), so it would read "[n]othing in this section shall be construed to impair the enforcement of . . . any . . . Federal *or State* criminal statute."
[161] https://www.eff.org/deeplinks/2013/07/state-ags-threaten-gut-cda-230-speech-protections
[162] http://www.forbes.com/sites/ericgoldman/2013/06/27/why-the-state-attorneys-generals-assault-on-internet-immunity-is-a-terrible-idea/; http://blog.ericgoldman.org/archives/2013/07/essay_explainin.htm
[163] http://aimgroup.com/2014/03/13/legislators-target-sex-trafficking-ads/
[164] 18 U.S.C. § 1591.

Backpage.com with respect to state statutes, and asserting that the statute would subject intermediaries to impossible monitoring and verification requirements of the sort that Section 230 was intended to prevent.[165] The American Civil Liberties Union and the Center for Democracy & Technology have also come out in opposition to this bill.[166]

Despite this, the bill passed the House of Representatives by a vote of 392-19, with twenty members not voting.[167] Several related bills are pending in the Senate.[168] Senate Bill 2536 – also called the "SAVE Act" but apparently not the Senate-introduced version of H.R. 4225 – is radically broader than the House bill, enacting strict record keeping requirements around all adult advertising, and expanding criminal liability for anyone hosting, selling, or promoting any ad that facilitates any state or federal sex trafficking, child sexual abuse, or assault on children statute.[169] The bill excludes Internet access service providers, Internet browsers, "external" information location tools, and telecommunications carriers. This works to exclude some online intermediaries, but critically – and in all likelihood, intentionally – not websites like Backpage.com or Craigslist.[170]

5. Conclusion

As the circumstances of Craigslist and Backpage.com illustrate, the presence of Section 230 concentrates criminal power for online activity to Congress, and leaves states with little ability to proscribe online behavior on their own. For all the public pressure that state authorities can bring to bear, Section 230 ultimately blocks their ability to suppress activity by using online intermediaries as a choke point. Calls by these intermediaries to instead cooperate to combat sex trafficking at the source, like those made by Craigslist during 2009 and 2010, have been rejected by state law enforcement. Accordingly, while image-conscious organizations such as Craigslist might decide to abandon such services, there are few alternatives available for states to take action against organizations like Backpage.com that refuse to succumb to that pressure.

For issues outside of sex trafficking, this situation is likely to continue. It appears that there is a lack of interest in Congress to grant state authorities broad discretion to impose criminal penalties on intermediaries for the conduct of their users, making a substantial amendment to Section 230 unlikely. Case-by-case solutions might, however, be reached at the federal level; as is the case of the pending SAVE Act. Federal statutory solutions are nevertheless more difficult to enact than state laws, not least because of the far greater public scrutiny that federal bills receive. It is likely that many online media organizations will raise challenges to the passage of the SAVE Act given the law's harsh criminal penalties and unclear boundaries, but as of yet only a few organizations have voiced opposition to the law.

---

[165] http://www.altweeklies.com/aan/proposed-bill-threatens-aan-members-right-to-free-speech/Article?oid=7622630
[166] https://cdt.org/blog/save-act-endangers-online-content-platforms/; https://www.aclu.org/blog/free-speech/anti-backpagecom-bill-will-shut-down-free-speech.
[167] *H.R. 4225: SAVE Act of 2014*, GOVTRACK, https://www.govtrack.us/congress/votes/113-2014/h222 (last viewed July 19, 2014).
[168] *See, e.g.*, Stop Exploitation Through Trafficking Act, S. 2599; End Trafficking Act of 2014, S. 2564; SAVE Act, S. 2536.
[169] *See* S. 2536 § 3.
[170] S. 2536 § 3.

B. Private Ordering to Respond to Copyright Concerns: YouTube's Content ID Program

As discussed at greater length in this document's Legal Landscape Primer, Section 512 of the Digital Millennium Copyright Act ("DMCA") makes it possible for online intermediaries ("OI"s) to have user-generated content ("UGC") on their platforms or networks that potentially infringes the copyrights of 3rd parties. However, unlike Section 230 of the Communications Decency Act, which, with minor exceptions, *completely* shields OI's from liability for defamatory UGC, and therefore eliminates for OIs the burden of either monitoring UGC or implementing a system for removal of such content with respect to defamation[171], Section 512 of the DMCA implements a regime in which online intermediaries can only shield themselves from liability if they adhere to certain practices. Section 512's criteria, in the aggregate, have become known as a "notice-and-takedown" regime, and the insulation from liability that the regime provides to intermediaries is the DMCA's "safe harbor." Online intermediaries who present or allow access to user-generated content that infringes copyright cannot be subjected to liability for that infringement as long as they comply with the tenets of Section 512.

Whether Section 512 "works" or not is a matter of much debate,[172] with some arguing that recent developments have proven that 512's mechanisms are totally inadequate for protecting the interests of copyright holders,[173] and others arguing that the balance Section 512 has struck errs too far on the side of protecting those same rights holders, at the expense of individuals and the public interest.[174] OIs themselves are also affected; with large-scale rights holders arguing OIs aren't doing enough to prevent infringement,[175] individual users arguing OI's treat those rights holders preferentially, on top of a recent explosion in the number of notices sent and acted on[176] and the attendant increased costs of compliance.[177] The resolution of these arguments notwithstanding, some online intermediaries have taken it upon themselves to go beyond the

---

[171] Eric Goldman, "Want To Scrub Google Search Results In The US? Tough–O'Kroley v. Fastcase | Technology & Marketing Law Blog," *Technology & Marketing Law Blog*, May 30, 2014, http://blog.ericgoldman.org/archives/2014/05/want-to-scrub-google-search-results-in-the-us-tough-okroley-v-fastcase.htm.

[172] Michael P. Murtagh, *The FCC, the DMCA, and Why Takedown Notices Are Not Enough*, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, November 15, 2009), http://papers.ssrn.com/abstract=1540200; Mike Masnick, "MPAA: Millions Of DMCA Takedowns Proves That Google Needs To Stop Piracy | Techdirt," *Techdirt.*, December 17, 2012, http://www.techdirt.com/articles/20121214/23441221394/mpaa-millions-dmca-takedowns-proves-that-google-needs-to-stop-piracy.shtml; Mark Schultz, "Time to Revise the DMCA: The Most Antiquated Part of the Copyright May Be One of the Newest-CICTP," *Tech Policy Daily*, accessed June 2, 2014, http://www.techpolicydaily.com/technology/time-revise-digital-millennium-copyright-act-antiquated-part-copyright-may-one-newest/.

[173] "RIAA Boss Says That The DMCA 'Isn't Working' Any More | Techdirt," *Techdirt.*, accessed June 2, 2014, http://www.techdirt.com/articles/20100824/00341310747.shtml.

[174] Niva Elkin-Koren, "Making Room for Consumers under the DMCA," *Berkley Technology Law Journal* 22, no. 3 Summer (February 2014); Matt Schruers, "5 Misconceptions We're Likely to Hear at Tomorrow's DMCA Hearing," 2014, http://www.project-disco.org/intellectual-property/31214-5-misconceptions-were-likely-to-hear-at-tomorrows-dmca-hearing/; Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, March 1, 2010), http://papers.ssrn.com/abstract=1577785.

[175] Schruers, "5 Misconceptions We're Likely to Hear at Tomorrow's DMCA Hearing."

[176] https://www.google.com/transparencyreport/removals/copyright/

[177] https://www.copyrightalliance.org/sites/default/files/resources/bruce-boyden-the-failure-of-the-dmca-notice-and-takedown-system.pdf

requirements of the DMCA and provide other mechanisms with which to manage and control content. It bears mentioning at the outset that these extra-legal mechanisms, while often modeled after the structures of the DMCA, are *not* part of it[178], not required in any way by law or regulation, and at least in theory have no effect on the true legal liability of the online intermediaries using them, liabilities that remain external to the private orderings in question.[179] The question is therefore, what external pressures, legal, regulatory, social and economic, have led to the creation and use of these extra-legal mechanisms?

This case study provides a short history of YouTube and then examines what is unquestionably the most elaborate, well-known, and (arguably) successful such private ordering mechanism for addressing copyright infringement: YouTube's "Content ID" system. Content ID continually monitors the majority of the videos on YouTube and upon finding a match, allows rights holders to decide whether to take the video down, place advertisements next to it, or simply monitor traffic to it. A key thread running throughout YouTube's history[180] is the tension between YouTube's reliance on arguably infringing copyrighted content to drive its success, its obvious need to avoid liability related to that same infringing content, and its need to maintain an adequately positive relationship both with its users, who upload the content that makes YouTube what it is, and with institutional copyright holders, whose intellectual property is interwoven with much of that content those users generate.

1. YouTube Is Created

YouTube was created in 2007 by several employees of PayPal. Within less than a year, it was popular enough to have 65,000 videos a day uploaded and to receive $12 million in venture capital funding from Sequoia.[181] Google purchased the company only months later for $1.65 billion.[182] Despite the confidence in the long-term viability of the YouTube business model that an infusion of venture capital and the subsequent purchase of the company clearly represented, the possibility of being held liable as secondary[183] copyright infringers loomed over the fledgling company from the first.[184] Negotiations with institutional content holders, who held the copyright

---

[178] "Latest Content ID Tool for YouTube," *Official Google Blog*, October 15, 2007, http://googleblog.blogspot.com/2007/10/latest-content-id-tool-for-youtube.html. ("Like many of these other policies and tools, Video Identification goes above and beyond our legal responsibilities.")

[179] See Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 40-41 (2d Cir. 2012) ("In other words, the safe harbor expressly disclaims any affirmative monitoring requirement—except to the extent that such monitoring comprises a "standard technical measure" within the meaning of § 512(i).")

[180] See the YouTube and Content ID Timeline, appendix B. p. 64.

[181] "A Brief History of YouTube - YouTube5Year," accessed May 11, 2014, https://sites.google.com/a/pressatgoogle.com/youtube5year/home/short-story-of-youtube; Megan Rose Dickey Feb 15 et al., "The 22 Key Turning Points In The History Of YouTube," *Business Insider*, February 15, 2013, http://www.businessinsider.com/key-turning-points-history-of-youtube-2013-2. See also the attached timeline, courtesy of Professor Terry Fisher's CopyrightX class.

[182] "Google Buys YouTube for $1.65 Billion," *Msnbc.com*, October 10, 2006, http://www.nbcnews.com/id/15196982/ns/business-us_business/t/google-buys-youtube-billion/.

[183] See this paper's Legal Landscape Primer, p. 9, for a discussion of secondary liability.

[184] "Google hopes to strike deals that will give it the rights to mainstream programming and also wipe away its potential liability for any violations of copyright law by YouTube so far." Geraldine Fabrikant and Saul Hansell, "Viacom Asks YouTube to Remove Clips," *The New York Times*, February 2, 2007, sec. Technology, http://www.nytimes.com/2007/02/02/technology/02cnd-tube.html; Anne, Greg Broache, Sandoval, "Viacom Sues Google over YouTube Clips - CNET News," March 17, 2007, http://news.cnet.com/Viacom-sues-Google-over-YouTube-clips/2100-1030_3-6166668.html.

in much of the content being uploaded to YouTube, began almost immediately. In 2006, YouTube was able to strike licensing deals with Warner Music, ABC, and NBC, three of the largest entities in the video media space,[185] despite the licensing fees that could be demanded for digital distribution of copyrighted works being derided as "digital pennies" that took the place of "analog dollars."[186] [187] [188] Viacom, another enormous player in the content industry,[189] also initially participated in negotiations, but ultimately refused to enter into any deal, and shortly thereafter asked YouTube to remove approximately 100,000 videos allegedly infringing its content from the site.[190]

Notably, according to Viacom, YouTube's business model at the time was predicated on providing access to copyrighted content. "They are saying we will only protect your content if you do a deal with us – if not, we will steal it."[191] Statements from Chad Hurley, one of YouTube's founders, seemed to confirm this, at least in part, [192] although the statements were arguably taken out of context.[193]

Unsurprisingly, YouTube officially took the opposite stance, specifically that it was both interested in licensing and willing to remove any infringing material upon being notified, according to the tenets of the DMCA's section 512, that it was present on their site.[194] In 2007 the DMCA was almost ten years old, and courts had already tested Section 512's provisions.[195] However, experts did not see existing law as clearly establishing Google/YouTube's immunity to liability,[196] identifying serious potential risks, at least with respect to the damages YouTube

---

[185] Candace Lombardi et al., "YouTube Cuts Three Content Deals - CNET News," *CNET*, accessed May 13, 2014, http://news.cnet.com/YouTube-cuts-three-content-deals/2100-1030_3-6123914.html.
[186] "Analog Dollars vs. Digital Pennies," *Edictive On Filmmaking*, accessed May 12, 2014, http://edictive.com/blog/analog-dollars-vs-digital-pennies/.

[188] While this criticism was perhaps true at one point, digital licensing fees continued to gain value and importance until they were an established part of the economics of the copyright ecosystem. "All3Media has hailed the end of the era of "digital pennies" as it forecasts that its digital activity will account for 11% of group profits this year." Alex Farber, "All3Media: Era of 'digital Pennies' Is Finally over," June 21, 2012, http://www.broadcastnow.co.uk/news/indies/all3media/all3media-era-of-digital-pennies-is-finally-over/5043559.article.
[189] A short list of the copyrighted properties Viacom owned at the time includes: MTV and its subsidiaries, Logo, Nickelodeon, Nick at Nite, Comedy Central, Spike TV, BET, TV Land, and Paramount films library, which included *titanic, Forrest Gump,* and the *Indiana Jones* and *Godfather* trilogies.
[190] Geraldine Fabrikant and Saul Hansell, "Viacom Asks YouTube to Remove Clips," *The New York Times*, February 2, 2007, sec. Technology, http://www.nytimes.com/2007/02/02/technology/02cnd-tube.html.
[191] Ibid.
[192] "YouTube Founder Pushed for Growth 'through Whatever Tactics, However Evil,'" *VentureBeat*, March 18, 2010, http://venturebeat.com/2010/03/18/youtube-founder-pushed-for-growth-through-whatever-tactics-however-evil/.
[193] Jason Kincaid, "Viacom Seems To Be Misrepresenting YouTube Founder's Call To 'Steal It!,'" *TechCrunch*, March 18, 2010, http://techcrunch.com/2010/03/18/viacom-may-be-misrepresenting-youtube-founders-call-to-steal-it/.
[194] Fabrikant and Hansell, "Viacom Asks YouTube to Remove Clips."
[195]https://ilt.eff.org/index.php/Copyright:_Digital_Millennium_Copyright_Act#Case_Law_Interpreting_the_DMCA_Safe_Harbor_Provisions
[196] Fabrikant and Hansell, "Viacom Asks YouTube to Remove Clips." ("John G. Palfrey Jr. , the executive director of the Berkman Center for Internet and Society at Harvard Law School, said Google may well be able to use this defense, but 'I don't think the law is entirely clear.' And if Google loses, 'the damages could get astronomically high,' he said.")

might have to pay if found to have contributed to infringement.[197] On the other hand, Viacom's course of action was seen as having its own dangers, including alienating[198] its customer base and missing an opportunity to be part of the burgeoning YouTube phenomenon. Both sides faced the burden of substantial legal fees,[199] potentially with nothing to show for them. Alongside all of this, the various media companies, including Viacom, were experimenting with their own competing distribution architectures and media platforms,[200] even as they licensed some or all of their material to YouTube and used the DMCA to take down other instances of it.[201] YouTube complied with the original set of takedown requests from Viacom,[202] but this was not enough to resolve things and, in early 2007, Viacom sued YouTube for $1 billion, alleging copyright infringement[203] and describing YouTube's activities as affecting "not just plaintiffs but the economic underpinnings of one of the most important sectors of the United States economy."[204] The suit came close on the heels of the United States Supreme Court's *Grokster* decision,[205] and the potential implications of a win for Viacom[206] were immediately apparent.[207]

It was against this backdrop, and with an eye toward heading off any future suits,[208] that YouTube began to develop its internal content monitoring system as early as the beginning of 2006.[209] From the start, this system ran alongside and complemented the mechanisms of Section

---

[197] As just one example calculation, if maximum statutory damages of $150,000 per willfully infringed work were awarded for a single day's worth of uploaded YouTube videos, the damages award would be in the billions.
[198] "Viacom Won't Soon Shed Image as Corporate Bully," *CNET*, July 8, 2008, http://www.cnet.com/news/viacom-wont-soon-shed-image-as-corporate-bully/.
[199] Liz Shannon Miller, "Google's Viacom Suit Legal Fees: $100 Million," *Gigaom*, July 15, 2010, http://gigaom.com/2010/07/15/googles-viacom-suit-legal-fees-100-million/.
[200] Fabrikant and Hansell, "Viacom Asks YouTube to Remove Clips." ("Just a few months ago, Viacom and Google were cozying up so successfully that Viacom struck a deal to have Google distribute clips from its shows on its Google Video service. The deal included an arrangement where the two companies would share revenue from adjacent advertising. Mr. Dauman yesterday characterized that deal as an "experiment."")
[201] "Official Blog: Broadcast Yourself," accessed July 15, 2014, http://youtube-global.blogspot.com/2010/03/broadcast-yourself.html.
[202] Louis Hau, "Viacom Demands YouTube Remove Videos," *Forbes*, accessed June 2, 2014, http://www.forbes.com/2007/02/02/viacom-youtube-google-markets-equity-cx_lh_0202markets20.html.
[203] Anne, Greg Broache, Sandoval, "Viacom Sues Google over YouTube Clips - CNET News," March 17, 2007, http://news.cnet.com/Viacom-sues-Google-over-YouTube-clips/2100-1030_3-6166668.html; Complaint Initial, "Viacom vs. YouTube," n.d., accessed May 12, 2014.
[204] Broache, Sandoval, "Viacom Sues Google over YouTube Clips - CNET News."; This sweeping proclamation of impending doom has strong echoes of then-President of the MPAA Jack Valenti's 1982 testimony to congress on the putative negative effects of the VCR on the movie industry. "I say to you that the VCR is to the American film producer and the American public as the Boston strangler is to the woman home alone."
[205] Notable for its framing of the "substantial non-infringing uses" test as to whether a particular technology could be banned or enjoined because of facilitating copyright infringement.
[206] Ars Staff, "Viacom v. YouTube Ruling Is a Bummer for Google and the UGC Community," *Ars Technica*, April 6, 2012, http://arstechnica.com/tech-policy/news/2012/04/second-circuit-ruling-in-viacom-v-youtube-is-a-bummer-for-google-and-the-ugc-community.ars.
[207] The Viacom suit itself only settled in 2014, after several appeals, and just prior to the next appearance by the parties in court. Of course during those years, YouTube only continued to grow and become more ubiquitous.
[208] Kevin J. Delaney, "YouTube to Test Software To Ease Licensing Fights," *Wall Street Journal*, June 13, 2007, sec. News, http://online.wsj.com/news/articles/SB118161295626932114?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB118161295626932114.html.
[209] Id; Kenneth Li and Eric Auchard, "YouTube to Test Video ID with Time Warner, Disney," *Reuters*, June 12, 2007, http://www.reuters.com/article/2007/06/12/us-google-youtube-idUSWEN871820070612; "Latest Content ID Tool for YouTube."

512[210], rather than taking their place. While the internal system had other names at the beginning[211], it quickly became known as Content ID. It is important to note that with respect to whether or not user uploaded videos infringed copyright, and whether YouTube could be held secondarily liable for any infringement, YouTube could have, and still can, rely solely on the safe harbors of the DMCA. Although early in its history there may have been pressure on YouTube to create a monitoring system in order to show their willingness to cooperate with rights holders, at this point, YouTube is under no obligation to run the Content ID system. But they do, presumably because they have decided it is better business practice to do so.

2. What Is Content ID?[212]

A complete examination of how Content ID has evolved over time is beyond the scope of this case study, but at its most fundamental level, it is an *automatic*[213] system with minimal human involvement,[214] in which:

- Content rights holders who qualify[215] may upload to YouTube's internal network copies of the material that they own and over which they wish to assert control. Rights holders indicate what they want to do with any content that matches their uploaded reference files. Options include: "block," in which the video is removed automatically; "track," in which the content owner can see how many views the video gets and from where; and critically, "monetize," in which YouTube will serve ads next to the user's video and the content owner will split the revenue from those ads 55-45 percent with YouTube[216];

- Any new content uploaded to YouTube is matched against the rights holder-uploaded reference database. If a match is found, the system presumes that this is an example of the user who uploaded the content having done so without permission from the rights holder, and therefore a potential copyright infringement.[217] Based on the rights holders' choice of block[218], track, or monetize, YouTube sends the uploading user a

[210] "YouTube's Content ID Disputes Are Judged by the Accuser - Waxy.org," accessed May 9, 2014, http://waxy.org/2012/03/youtube_bypasses_the_dmca/. ("[The DMCA] wasn't perfect, by any means, but it was fair. Disputes could always be appealed, and both parties were given equal power. And if a claimant lied about owning the copyright to the material in question, they could face perjury charges.")

[211] "Latest Content ID Tool for YouTube."

[212] See here for a comprehensive internal document explaining the entire ContentID process. Carlos Pacheco, "YouTube Content ID Handbook - Google," (Technology, 19:41:05 UTC), http://www.slideshare.net/carlospacheco74/you-tube-content-id-handbook.

[213] The lack of human involvement is a critical piece, as it is this which not only makes it possible for the system to keep up with the flood of material being uploaded to YouTube but also which means that edge cases and false positive results are more common, and difficult to subject to human review. YouTube does have a parallel human review process whereby users can flag videos as objectionable, and they will then be tracked for review by a human being, as well as a "super-flagger" program within the larger crowdsourced version.

[214] Human beings could never review all of YouTube's material, but depending on the nature of the Content ID flag, a particular video may get pushed to a "manual review" queue. See

[215] "Qualifying for Content ID - YouTube Help," accessed May 9, 2014, https://support.google.com/youtube/answer/1311402.

[216] "The Hidden Costs of YouTube's Controversial Revenue Split," *The Daily Dot*, accessed July 2, 2014, http://www.dailydot.com/opinion/youtube-content-creator-split/.

[217] "How Content ID Works - YouTube Help," accessed May 9, 2014, https://support.google.com/youtube/answer/2797370?hl=en.

[218] Blocking is "not the DMCA" and does not result in a strike

> notification that an upload of theirs has triggered the system, and what the consequences are. Repeat violators have their account terminated.[219] At no point is a human being involved – to determine fair use, for example – although human reviewers may watch videos as part of other parts of YouTube's video review processes, for example when users "flag" videos.[220]

The Content ID process therefore owes much to the DMCA's mechanisms of notice-and-takedown followed by counter-notification. Rights holders (or their uploaded reference files) "notify" YouTube of a possible infringement, and YouTube acts on the material in question. The key differences between the two processes are: with Content ID, content owners do not have to proactively police YouTube for their content in order to notify YouTube, because the scanning for matches takes place automatically; rights holders have more choices available to them than just a takedown; and, at least in theory, the consequences for the content-posting users in question are less serious.[221] Further, the DMCA and its mechanisms are always available as well, either during or after the ContentID process. At any point in the Content ID process, a copyright holder has the opportunity to file a DMCA notice to take the material down. Additionally, if a user challenges the Content ID outcome, it is possible that a DMCA notice will be a rights holder's only remaining option. Therefore, the possibility of invoking Federal copyright law always hangs over any of Content ID's disputes, but this is a blunt instrument, with none of the nuances or possible beneficial outcomes that Content ID offers.

Initially, a YouTube user who received a Content ID notification had only one response, to "dispute" the claim.[222] A dispute from a user originally resulted in a removed video being replaced or monetization being restored to the user, and the content owner being notified of the dispute. The owner would then have the binary option of allowing the video to remain up, or filing a DMCA notice to take it down. Later, the owner was given the ability to "reject" the dispute, which left the video down and the user with no further recourse for some claims.[223] [224] In 2012, YouTube introduced the current – theoretically more user-friendly – appeals process, to mixed reaction.[225]

---

[219] Note the similarities to Section 512(i)(1)(A)'s statement about the service provider's needing to have a "policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers;"

[220] "Flagging Content - YouTube Help," accessed July 13, 2014, https://support.google.com/youtube/answer/2802027.

[221] "What Is a Content ID Claim? - YouTube Help," accessed May 9, 2014, https://support.google.com/youtube/answer/6013276?hl=en. ("In most cases, getting a Content ID claim isn't a bad thing for your YouTube channel. It just means, 'Hey, we found some material in your video that's owned by someone else.'")

[222] Patrick McKay, "Victory! YouTube Reforms Content ID Dispute Process," October 4, 2012, http://fairusetube.org/articles/25-content-id-victory.

[223] "Official Blog: Improving Content ID," October 3, 2012, http://youtube-global.blogspot.com/2012/10/improving-content-id.html.

[224] "YouTube Refuses to Honor DMCA Counter-Notices," accessed June 17, 2014, http://fairusetube.org/articles/27-youtube-refuses-counter-notices.

[225] McKay, "Victory! YouTube Reforms Content ID Dispute Process"; "Official Blog: Improving Content ID."

Currently, a user whose content triggers a Content ID warning may first "dispute" it.[226] The relevant copyright owner may then release the claim, uphold the claim, or take the video down by submitting a DMCA notice. If the owner releases the claim, the video goes back up and the process ends. If the owner upholds the claim, the user's dispute has been "rejected" and the user may then "appeal" that decision, placing the ball back in the copyright owner's court.[227] However, a user can appeal only three rejections at once, and that requires that the user's account be in good standing.[228] A user with even a moderate number of videos on YouTube, to say nothing of hundreds, could easily and quickly receive more Content ID claims than they could appeal. There is therefore a clear incentive on the part of complaining rights holders to use Content ID over the DMCA, since an un-appealed notification essentially ends the process in a way that favors the rights holder, while a DMCA notice can be counter-noticed, etc.

After an appeal, the owner has thirty days to respond by either releasing the video as above, or issuing a formal DMCA request, thereby taking the alleged infringement out of YouTube's private ordering and into the actual tenets of federal copyright law. However, Content ID may remain involved, albeit for other user content. Notably, if a user receives a DMCA notice, they receive a "strike" on their account.[229] Having a "strike" means that the user cannot appeal a Content ID rejection, and three strikes can result in the loss of an account, with no way to regain it or its content.[230] Strikes can be removed by waiting for six months, attending YouTube's somewhat ridiculous[231] "copyright school"[232] or by successfully submitting a counter notice. Notably, and apropos the balancing of interests that copyright law and the DMCA are meant to accomplish, there does not appear to be any corresponding set of accumulating penalties for owners whose Content ID claims are eventually dropped.[233] However, YouTube does assert that it will remove owners from the Content ID partner system for systematic misuse or abuse.[234]

It is quite easy to make a list of high-profile failures of the Content ID system, failures that have serious consequences for culture,[235] [236] [237] civic participation,[238] [239] [240] an educated public,[241] and

---

[226] "Dispute a Content ID Claim - YouTube Help," accessed May 9, 2014, https://support.google.com/youtube/answer/2797454?hl=en. ("After you appeal a rejected dispute, the copyright owner has 30 days to respond. If they don't respond within 30 days, their claim on your video will expire, and you don't need to do anything.")

[227] Carlos Pacheco, "YouTube Content ID Handbook - Google," (Technology, 19:41:05 UTC), http://www.slideshare.net/carlospacheco74/you-tube-content-id-handbook; "Dispute a Content ID Claim - YouTube Help." slide 79

[228] Which requires that a user have no Community Guidelines strikes, no copyright strikes and no more than one video blocked worldwide by Content ID; See "Dispute a Content ID Claim"

[229] "A Guide to YouTube Removals," *Electronic Frontier Foundation*, accessed May 9, 2014, https://www.eff.org/issues/intellectual-property/guide-to-youtube-removals.

[230] Strikes can be erased with either the passage of time or by attending YouTube's bizarre "copyright school" https://www.youtube.com/copyright_school

[231] elisa, "Help Fix YouTube's Copyright School Fail," *Political Remix Video*, April 22, 2011, http://www.politicalremixvideo.com/2011/04/22/help-fix-youtubes-copyright-school-fail/.

[232] "YouTube Copyright School," accessed July 15, 2014, https://www.youtube.com/copyright_school.

[233] Carlos Pacheco, "YouTube Content ID Handbook - Google," 19:41:05 UTC.

[234] Id., slides 43, 48, 59

[235] "Major Labels Claim Copyright Over Public Domain Songs; YouTube Punishes Musician | Techdirt," *Techdirt.*, accessed July 1, 2014, https://www.techdirt.com/articles/20120827/22533320172/major-labels-claim-copyright-over-public-domain-songs-youtube-punishes-musician.shtml.

more. Some false positives are simply ridiculous,[242] but some threaten the public domain.[243] It can be argued that the very fact that failures like this make the news is because they are proportionately rare, although hard data on ContentID's true error rate is lacking, perhaps because what counts as an "error" is not universally agreed upon. On the other hand, the seemingly low occurrence of error may be because the majority of users whose legitimate content is adversely affected by Content ID simply allow it to remain down because they are reluctant to engage with the process for whatever reason or because they don't know that processes for redress exist at all. It's equally simple to make a list of Content ID-related successes[244], even not including the astonishing economic success of YouTube itself.[245] But whether positive, negative, or more complex, the implications of, and outcomes associated with, a vast automatic private ordering system like Content ID are both far-reaching and multi-faceted. This case study will examine some of them through a variety of different interpretive lenses.

---

[236] Brian Kamerer | May 24th and 2012, "An Open Letter to Jay Leno About Stealing My Video and Then Getting It Removed From YouTube," *Splitsider*, accessed July 1, 2014, http://splitsider.com/2012/05/an-open-letter-to-jay-leno-about-stealing-my-video-and-then-getting-it-removed-from-youtube/.

[237] "How I End up with YouTube Copyright Claims on My Own Songs | Chris Zabriskie | Composer," accessed July 1, 2014, http://chriszabriskie.com/2013/04/how-i-end-up-with-youtube-copyright-claims-on-my-own-songs/.

[238] "Telemundo & Univision Copyright Claim On YouTube Takes Down US Congressional Appropriations Hearing | Techdirt," *Techdirt.*, accessed July 1, 2014, https://www.techdirt.com/articles/20140331/11022126751/telemundo-univision-copyright-claim-youtube-takes-down-us-congressional-appropriations-hearing.shtml.

[239] Ryan Singel, "YouTube Flags Democrats' Convention Video on Copyright Grounds | Threat Level," *WIRED*, September 5, 2012, http://www.wired.com/2012/09/youtube-flags-democrats-convention-video-on-copyright-grounds/.

[240] Timothy B. Lee, "Music Publisher Uses DMCA to Take down Romney Ad of Obama Crooning," *Ars Technica*, July 16, 2012, http://arstechnica.com/tech-policy/2012/07/major-label-uses-dmca-to-take-down-romney-ad-of-obama-crooning/.

[241] Alex Pasternack, "NASA's Mars Rover Crashed Into a DMCA Takedown," *Motherboard*, accessed July 1, 2014, http://motherboard.vice.com/blog/nasa-s-mars-rover-crashed-into-a-dmca-takedown.

[242] "YouTube Content ID Under Fire As False Copyright Claims Abound," *SocialTimes*, accessed July 1, 2014, http://socialtimes.com/youtube-content-id-false-copyright-claims_b90469. The birdsong on a video of a nature walk triggered a match to content owned by Rumblefish, who when first notified of the error, nevertheless rejected the dispute!

[243] "Major Labels Claim Copyright Over Public Domain Songs; YouTube Punishes Musician | Techdirt"; "YouTube Taking Down Public Domain Works? | Techdirt," *Techdirt.*, accessed July 10, 2014, https://www.techdirt.com/articles/20091028/0306106704.shtml; "How Google's ContentID System Fails At Fair Use & The Public Domain | Techdirt," *Techdirt.*, accessed May 9, 2014, http://www.techdirt.com/articles/20120808/12301619967/how-googles-contentid-system-fails-fair-use-public-domain.shtml.

[244] Christopher Zoia, "This Guy Makes Millions Playing Video Games on YouTube," *The Atlantic*, March 14, 2014, http://www.theatlantic.com/business/archive/2014/03/this-guy-makes-millions-playing-video-games-on-youtube/284402/; Amanda Holpuch, "Harlem Shake: Baauer Cashes in on Viral Video's Massive YouTube Success," *The Guardian*, February 19, 2013, sec. Technology, http://www.theguardian.com/technology/2013/feb/19/harlem-shake-baauer-youtube-success; "How to Make Money on YouTube: 101 Monetization Tips | MonetizePros," accessed May 9, 2014, http://monetizepros.com/blog/2013/101-ways-to-make-money-with-youtube-web-videos/; "Musician Alex Day Explains How He Beat Justin Timberlake In The Charts Basically Just Via YouTube | Techdirt," *Techdirt.*, March 25, 2013, http://www.techdirt.com/blog/casestudies/articles/20130324/01115322434/musician-alex-day-explains-how-he-beat-justin-timberlake-charts-basically-just-via-youtube.shtml.

[245] Ryan Lawler, "YouTube Has Found Its Business Model, And Is Paying Out Hundreds Of Millions Of Dollars To Partners," *TechCrunch*, accessed May 14, 2014, http://techcrunch.com/2012/07/19/youtube-business-model/.

3. What Can An Examination Of YouTube And Content ID Tell Us About Online Intermediaries And Private Ordering?

YouTube is, at its root, constructed by the content of its users, and therefore has an almost Protean[246] nature. YouTube is an extremely powerful platform and tool, in part because of its audio-visual nature[247] and has arguably evolved to become what its users need it to be, though of course in some tension with what YouTube itself is willing and able to allow itself to be.[248] However, because it actively occupies the space between content owners and users, YouTube is arguably much more than a simple UGC platform. The overwhelming market share,[249] ubiquity, and ease of use of the YouTube platform have made it an essential tool for not only private or recreational communication and uses, but public ones as well.[250] YouTube is a paradigmatic example of a "social media" OI.[251] Videos on YouTube can be breaking news,[252] and also provide the raw material underlying many articles and broadcasts, but clearly YouTube is not a traditional journalistic medium.[253] Is YouTube a search engine? As a "simple" database of videos, it may not appear to be at first, but it is unquestionably used and thought of as one, and an enormous one at that.[254] Although not a traditional "blogging" site by most meanings of that word, "vlogging" is a burgeoning trend,[255] and more and more popular users and channels on YouTube are simply users sharing their thoughts and ideas, rather than "constructed"

---

[246] http://www.perseus.tufts.edu/hopper/text?doc=Perseus:text:1999.01.0180:text=Ion:section=541e&highlight=proteus

[247] Combined bandwidth into the brain for eyes and ears exceeds 10 MBps http://www.newscientist.com/article/dn9633-calculating-the-speed-of-sight

[248] "The street finds its own uses for things" "William Gibson, "Burning Chrome" *Omni* in July 1982; See also Ann Balsamo, arguing that when it comes to designing new technologies, we, the designers, need to leave the potential of those technologies as open as possible. Video available at http://cyber.law.harvard.edu/node/4382 ; Last viewed Jan. 12, 2009

[249] "YouTube Leads US Online Video Market with 28% Market Share," *MarketingCharts*, accessed July 11, 2014, http://www.marketingcharts.com/television/youtube-leads-us-online-video-market-with-28-market-share-2588/.

[250] Katharine Q. Seelye, "New Presidential Debate Site? Clearly, YouTube - New York Times," June 13, 2007, http://www.webcitation.org/mainframe.php; Kristal Leah Curry, "YouTube's Potential as a Model for Democracy: Exploring Citizentube for 'Thick' Democratic Content," *Journal of Curriculum Theorizing* 28, no. 1 (April 18, 2012), http://journal.jctonline.org/index.php/jct/article/view/121; "Facebook, Twitter, YouTube—and Democracy," 2010, http://www.aaup.org/article/facebook-twitter-youtube%E2%80%94and-democracy; "Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Political Speech | Center for Democracy & Technology," accessed July 8, 2014, https://cdt.org/insight/campaign-takedown-troubles-how-meritless-copyright-claims-threaten-online-political-speech/; Singel, "YouTube Flags Democrats' Convention Video on Copyright Grounds | Threat Level"; Curry, "YouTube's Potential as a Model for Democracy"; "CitizenTube: What Is Democracy? The State Department and YouTube Put It to a Vote," accessed May 14, 2014, http://www.citizentube.com/2009/05/what-is-democracy-state-department-and.html.

[251] "Top 10 Social Networking Sites by Market Share of Visits [January 2013]," *DreamGrow Social Media*, accessed July 11, 2014, http://www.dreamgrow.com/top-10-social-networking-sites-by-market-share-of-visits-january-2013/.

[252] https://www.youtube.com/news

[253] Pew Research Center's Journalism Project Staff, "YouTube & News," *Pew Research Center's Journalism Project*, accessed July 15, 2014, http://www.journalism.org/2012/07/16/youtube-news/.

[254] "YouTube: The 2nd Largest Search Engine (Infographic)," accessed July 11, 2014, http://www.mushroomnetworks.com/infographics/youtube---the-2nd-largest-search-engine-infographic.

[255] "In-Depth Statistics on Online Video Sharing and Engagement - Part I," accessed July 11, 2014, http://www.sysomos.com/reports/video/. ("YouTube is the most popular video-sharing service used by bloggers attracting 81.9% of all embedded videos")

entertainment.[256] It has even become possible to purchase content on YouTube.[257] The platform's identity as an intermediary is therefore one that blurs category lines, making the way in which it negotiates the potential liability for its content all the more illuminating.

The presence of ContentID means that YouTube's liability for, and handling of, the user-generated content that gives the site its unique qualities is subject to more pressures than just the largely ex post law of the DMCA. Other influences include the markets, in the form of YouTube's need to succeed as a business and the normative pressures of its users[258] and also the algorithmic decisions that underlie Content ID's computer code and produce its outcomes.

From a liability perspective, YouTube is subject only to the DMCA and, if appropriate, CDA 230. YouTube could choose to rely solely on the DMCA's mechanisms to police its content.[259] The DMCA is for the most part an "enabling" *ex post* regime. In contrast, Content ID is an *ex ante* regime that, at first glance, places additional net restrictions and costs on YouTube. But Content ID is a voluntary addition. Why then has YouTube chosen to invest substantial resources in Content ID if it is under no obligation to do so?

Content ID has been part of YouTube since nearly the beginning. Arguably, YouTube started Content ID as a direct response to the threat of the then-ongoing Viacom litigation,[260] and it seems reasonable to suggest that if there had been no lawsuit and no looming copyright liability (for example, if the DMCA somehow completely immunized OSPs for all user postings under all circumstances) that YouTube would have had little incentive to innovate or investigate new ways to monitor and police its content. Professor Terry Fisher[261] has described Content ID as a way that YouTube could show both the court and the public that it was trying to do the right thing regarding its legal obligations, as part of a larger strategy that would enable it to survive.[262] But Content ID quickly became much more than just reputation management, especially as YouTube continued to grow and to gain an audience.[263] In contrast to the blunt (but arguably more fair) instrument that was the DMCA, Content ID's "block/track/monetize" gave rights holders more nuanced choices than "up", "down" or "lawsuit", which in turn made it possible for users and rights holders to innovate into the new spaces provided along a variety of axes. Although in

[256] See, e.g. https://en.wikipedia.org/wiki/Jenna_Marbles. Note though that as "average" YouTube users become more popular, the production values of their videos tend to increase.
[257] Jennifer Van Grove, "YouTube Expands Click-to-Buy, Takes Over Your Videos," *Mashable*, January 21, 2009, http://mashable.com/2009/01/21/youtube-click-to-buy-overlay-ads/; "I Clicked to Buy and I Liked It," *Official Google Blog*, accessed June 3, 2014, http://googleblog.blogspot.com/2008/10/i-clicked-to-buy-and-i-liked-it.html.
[258] Liz Shannon Miller, "Should YouTubers Launch New Platforms to Compete with YouTube?," June 9, 2013, http://gigaom.com/2013/06/09/should-youtubers-launch-new-platforms-to-compete-with-youtube/; "Union For Gamers," *Union For Gamers*, accessed June 9, 2014, http://www.unionforgamers.com/.
[259] "Viacom v. YouTube: How a District Court Saved Free Speech on the Internet," *American Civil Liberties Union of Washington*, July 6, 2010, https://aclu-wa.org/blog/viacom-v-youtube-how-district-court-saved-free-speech-internet.; https://www.eff.org/files/filenode/viacom_v_youtube/YouTubeAmicusBriefFINAL.pdf
[260] Verne Kopytoff, Chronicle Staff Writer, "Copyright Questions Dog YouTube / Deals with Entertainment Industry Limit Site's Liability," *SFGate*, October 27, 2006, http://www.sfgate.com/business/article/Copyright-questions-dog-YouTube-Deals-with-2485823.php#src=fb.
[261] WilmerHale Professor of Intellectual Property Law, Harvard Law School
Director, Berkman Center for Internet & Society https://cyber.law.harvard.edu/people/tfisher
[262] See right-hand side of H. Appendix C: Business Strategies Mind-Map at appendix C, p 65; CopyX lecture 11.2 at https://www.youtube.com/watch?v=UnqXnZyLRUw&feature=youtu.be
[263] A 2009 survey found that users found online video on YouTube more than any other site, by a substantial percentage.

some ways it may seem more restrictive, and may well be, from a given individual user's perspective, Content ID is, broadly, a more enabling regulatory regime than the DMCA. Other UGC platforms, such as SoundCloud, have recognized Content ID's success and have emulated it, sometimes for exactly the same reasons,[264] and unsurprisingly, with many of the same controversies.[265] However, many of Content ID's affordances also have a negative side, a side that almost always has to do with the difficulty of how to effectively scale individual problem-solving and fact-specific inquiry that a user needs to the exigencies of YouTube's immense size and volume.

4. What Has Content ID Made Possible?

i. Social and Cultural Impacts

Remix culture thrives on YouTube, although there is a great deal of "original" content as well. Content ID gives rights holders the ability to curate which remixes of their material they are willing to tolerate, a new form of (indirect) brand management.[266] [267] Some rights holders don't attempt to curate at all, seeing each reuse of their material as free publicity, facilitating greater popularity for the material in question.[268] In parallel, users have access to a much wider range of copyrighted materials with which to remix and create new content, materials that the use of which would previously have caused their videos to be removed under the DMCA. When user-generated content that arguably infringes copyright remains available to digital bricoleurs, there is more freedom to use the raw materials of popular culture to make commentary, have fun, or simply to participate, and works that incorporate those materials can remain public and reach a much wider audience. On the other hand, many uses of content would, if challenged in court, be ultimately deemed fair use, and therefore not infringement. Relying on Content ID and its automatic processes means that the fair use analysis never takes place, and that a great deal of content that should actually remain online is blocked under Content ID.[269]

However, the democratization of access that the YouTube platform and medium represent – the lack of traditional obstacles and gatekeepers – has been a boon to those who might otherwise have struggled to get their voices heard.[270] In addition, it has facilitated the formation of new

---

[264] "SoundCloud » Q&A: Our New Content Identification System," accessed July 10, 2014, http://blog.soundcloud.com/2011/01/05/q-and-a-content-identification-system/; "After Heavy Threats, SoundCloud Agrees to Label Licensing Talks...," *Digital Music News*, accessed July 10, 2014, http://www.digitalmusicnews.com/permalink/2014/03/27/soundcloudlicenses; "Soundcloud Doing a Deal With Record Labels Not to Get Sued | TorrentFreak," accessed July 11, 2014, https://torrentfreak.com/soundcloud-doing-a-deal-with-record-labels-not-to-get-sued-140711/.

[265] "Universal Music Can Delete Any SoundCloud Track Without Oversight | TorrentFreak," accessed July 11, 2014, http://torrentfreak.com/record-labels-can-remove-soundcoud-tracks-without-oversight-140703/.

[266] Stuart Dredge, "Disney's YouTube Deal Is a Real Game Changer," *The Guardian*, March 29, 2014, sec. Technology, http://www.theguardian.com/technology/2014/mar/30/disney-youtube-deal-game-changer.

[267] "Copyright And The Harlem Shake: Selective Enforcement | Techdirt," *Techdirt.*, accessed July 10, 2014, https://www.techdirt.com/articles/20130218/23563522021/copyright-harlem-shake-selective-enforcement.shtml.

[268] "Number Ones - Psy 'Gangnam Style,'" *TheVine.com.au*, accessed July 10, 2014, http://www.thevine.com.au/music/news/number-ones-psy-gangnam-style-20121002-250944/.

[269] "How Google's ContentID System Fails At Fair Use & The Public Domain | Techdirt."

[270] Hayley Tsukayama, "In Online Video, Minorities Find an Audience," *Washington Post*, April 20, 2012, http://www.washingtonpost.com/business/economy/in-online-video-minorities-find-an-audience/2012/04/20/gIQAdhliWT_story.html.

bonds of community and organization, both social[271] [272] and commercial,[273] groups whose fortunes may in part rise and fall with YouTube's.[274] YouTube is increasingly a space in which political discourse takes place, albeit still in parallel to more traditional channels. [275] [276] [277] [278]

Conversely, the same size and breadth that makes YouTube such a powerful platform means that as it deploys Content ID and responds to the DMCA, it must balance the interests of a much wider spectrum of users, interests of whom may often inadvertently come into conflict. Speech on YouTube may be censored[279] deliberately[280] for personal,[281] commercial[282], and political[283] reasons. Perhaps even more importantly, accidental censorship may occur as a result of poorly targeted Content ID matching, or creating a collision with unknowing and likely indifferent commercial interests.[284] As an example of how the application of Content ID can have far-

[271] Clement Chau, "YouTube as a Participatory Culture," *New Directions for Youth Development* 2010, no. 128 (December 1, 2010): 65–74, doi:10.1002/yd.376; Bryan Mueller, "Participatory Culture on YouTube: A Case Study of the Multichannel Network Machinima," August 2013; "Union For Gamers."
[272] Erik Kain, "YouTube Responds To Content ID Crackdown, Plot Thickens," *Forbes*, December 17, 2013, http://www.forbes.com/sites/erikkain/2013/12/17/youtube-responds-to-content-id-crackdown-plot-thickens/.
[273] Michael Carney On August 15 and 2013, "AdRev Launches ContentID.com, Brings Music Rights Management to the YouTube Masses," *PandoDaily*, August 15, 2013, http://pando.com/2013/08/15/adrev-launches-contentid-com-brings-music-rights-management-to-the-youtube-masses/. ("use the illegally uploaded uses of their client's IP as distribution and drive audience to that content to increase ad-based monetization.
Secondly, AdRev and ContentID.com aid their clients in "commercializing" their IP through micro synchronization partnerships with YouTube MCNs including Maker Studios, FullScreen, Big Frame, Bent Pixels, MiTu, and others, and also through uploading this content to iTunes and Amazon."
[274] Staff, "Viacom v. YouTube Ruling Is a Bummer for Google and the UGC Community."
[275] Seelye, "New Presidential Debate Site?"
[276] Erin F. Dietel-McLaughlin, "Remediating Democracy: YouTube and the Vernacular Rhetorics of Web 2.0" (Bowling Green State University, 2010), https://etd.ohiolink.edu/ap/10?0::NO:10:P10_ACCESSION_NUM:bgsu1275323561.
[277] "CitizenTube," accessed May 14, 2014, http://www.citizentube.com/.
[278] "Campaign Takedown Troubles."
[279] https://en.wikipedia.org/wiki/Censorship_by_YouTube#YouTube;
[280] "Why Yes, Copyright Can Be Used To Censor, And 'Fair Use Creep' Is Also Called 'Free Speech' | Techdirt," *Techdirt.*, accessed July 13, 2014, https://www.techdirt.com/articles/20130726/12394323961/why-yes-copyright-can-be-used-to-censor-fair-use-creep-is-also-called-free-speech.shtml; Cory Doctorow at 3:00 pm Sat, Feb 15, and 2014, "AIDS Deniers Use Bogus Copyright Claims to Censor Critical YouTube Videos," *BoingBoing*, accessed July 13, 2014, http://boingboing.net/2014/02/15/aids-deniers-use-bogus-copyrig.html; "Hollywood Studios Censor Pirate Bay Documentary | TorrentFreak," accessed July 13, 2014, http://torrentfreak.com/hollywood-studios-take-down-pirate-bay-documentary-130519/.
[281] "Copyright As Censorship: Using The DMCA To Take Down Websites For Accurately Calling Out Racist Comments | Techdirt," *Techdirt.*, accessed July 13, 2014, https://www.techdirt.com/articles/20130925/01355924650/copyright-as-censorship-using-dmca-to-take-down-websites-accurately-calling-out-racist-comments.shtml.
[282] "Rotolight Uses DMCA To Censor Review They Didn't Like, Admits To DMCA Abuse For Censorship | Techdirt," *Techdirt.*, accessed July 13, 2014, https://www.techdirt.com/articles/20130730/17572624008/rotolight-uses-dmca-to-censor-review-they-didnt-like-admits-to-dmca-abuse-censorship.shtml.
[283] "State Censorship by Copyright? Spanish Firm Abuses DMCA to Silence Critics of Ecuador's Government," *Electronic Frontier Foundation*, accessed July 13, 2014, https://www.eff.org/deeplinks/2014/05/state-censorship-copyright-spanish-firm-abuses-DMCA.
[284] "Warner Bros. Censorship of Greenpeace LEGO Video Backfires | TorrentFreak," accessed July 11, 2014, https://torrentfreak.com/warner-bros-censorship-of-greenpeace-lego-video-backfires-140711/; *My Own Game Has Been Flagged by YouTube!*, 2013, https://www.youtube.com/watch?v=wJKhGl5DIDU&feature=youtube_gdata_player; "Record Label Reaches Settlement With Lessig; Promises To Revamp Abusive DMCA Takedown Policies -- Chilling Effects

reaching and substantial effects on an entire subculture, business model, and economic ecosystem, see the extensive coverage of the December 2013 "multichannel network" controversy,[285] wherein thousands of users simultaneously received numerous Content ID notices virtually overnight, many of which were from seemingly unrelated third party content holders.[286] See also more recent controversies having to do with YouTube's introduction of YouTube Music Key - "essentially a cosmetically enhanced YouTube reinvented as a free and paid subscription service like Spotify."[287]

ii. Legal and Regulatory Innovation

One clear difference between what is possible with a private ordering system like Content ID, as compared to federal legislation like the DMCA, is the potential speed of adaptation. YouTube itself has only been in existence for seven years, but Content ID has already gone through several major iterations.[288] In contrast, the DMCA, the most recent major change to copyright law, is fifteen years old, and the U.S. Congress is only just now under massive pressure from a variety of constituencies, acknowledging that current copyright law – and especially the DMCA – are perhaps not the best fit for the realities of the networked digital age.[289] Being able to change as needed may be more work for YouTube, in contrast to standing on the floor of the DMCA's safe harbors, but it makes YouTube more nimble, and less reliant on government to protect its existing business model.[290]

With a private schema, OIs like YouTube at least have the opportunity to do a better job of managing the evolving needs of their users, whether individual or institutional. YouTube will

---

Clearinghouse," accessed July 13, 2014, https://www.chillingeffects.org/news.cgi?NewsID=819; Singel, "YouTube Flags Democrats' Convention Video on Copyright Grounds | Threat Level"; "How YouTube Lets Content Companies 'claim' NASA Mars Videos | Ars Technica," accessed May 8, 2014, http://arstechnica.com/tech-policy/2012/08/how-youtube-lets-content-companies-claim-nasa-mars-videos/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+arstechnica/index+%28Ars+Technica+-+All+content%29&utm_content=Google+Reader.

[285] Paul Tassi, "The Injustice Of The YouTube Content ID Crackdown Reveals Google's Dark Side," *Forbes*, accessed May 14, 2014, http://www.forbes.com/sites/insertcoin/2013/12/19/the-injustice-of-the-youtube-content-id-crackdown-reveals-googles-dark-side/; Mike Masnick, "Dan Bull Takes On YouTube's ContentID Changes, Stolen Revenue, With A Diss Track | Techdirt," *Techdirt.*, January 3, 2014, http://www.techdirt.com/articles/20140102/17424525757/dan-bull-takes-youtubes-contentid-changes-stolen-revenue-with-diss-track.shtml.

[286] "What People Don't Get About Content ID," accessed June 11, 2014, http://edwardspoonhands.com/post/71433962019/what-people-dont-get-about-content-id.

[287] Sarah Manning and Jeff Boxer, "What Zoe Keating's Battle With YouTube Really Means For Indie Artists," c3action, February 17, 2014, http://www.c3action.org/

[288] "History of Content Management - YouTube5Year," accessed May 11, 2014, https://sites.google.com/a/pressatgoogle.com/youtube5year/home/history-of-copyright.

[289] "U.S. Copyright Office: The Register's Call for Updates to U.S. Copyright Law," accessed July 11, 2014, http://www.copyright.gov/regstat/2013/regstat03202013.html; Schruers, "5 Misconceptions We're Likely to Hear at Tomorrow's DMCA Hearing"; "Copyright Hearing Recap: DMCA Notice & Takedown | Future of Music Coalition," accessed July 11, 2014, http://futureofmusic.org/blog/2014/03/20/copyright-hearing-recap-dmca-notice-takedown.

[290] William Patry, *How to Fix Copyright* (Oxford University Press, 2011); "ISP CEO Slams Copyright Law and Outdated Business Models | TorrentFreak," accessed July 13, 2014, https://torrentfreak.com/isp-ceo-slams-copyright-law-and-outdated-business-models-110815/.

obviously never be able to satisfy all of its constituencies all of the time,[291] but even when they get it wrong, a fix can be implemented[292] far more rapidly than a new law can be passed. YouTube's success with Content ID is already being emulated by other OIs who must balance their users' interests against those of the content industry, and who have previously faced similar lawsuits as they while engaging in licensing talks.[293] The outstanding questions then become the extent to which the voices of individual users can be heard over those of powerful business interests, and the extent to which YouTube will make its private ordering transparent. Ideally, all of the involved parties should agree to the rules under which they will interact,[294] and, for now, YouTube users seem to be something of an afterthought.[295] It may still prove to be the case that the public interest is best served through law's public ordering.

Somewhat more speculatively, it seems that adding the private layer of Content ID may mean a reduction in the number of infringement-based conflicts that actually make it to court. Why would a rights holder file suit, or even threaten, if the material in question can be easily blocked or monetized through Content ID with minimal effort? This should in theory result in a smaller workload for federal courts, at least with respect to copyright lawsuits. Or it may mean less DMCA-related case law, and the stagnation of jurisprudence in that area. Regardless, this is a worthy topic for future research. Compare the massive copyright litigation campaign of Malibu Media, a rights holder that during one year was responsible for filing nearly 40% of all U.S. copyright lawsuits.[296]

---

[291] "YouTube Fails In Explaining Flood Of Takedowns For Let's Play Videos | Techdirt," *Techdirt.*, accessed June 11, 2014, https://www.techdirt.com/articles/20131211/17365325537/youtube-fails-explaining-flood-takedowns-lets-play-videos.shtml; Mark Sweeney, "YouTube Accused of Trying to Strong-Arm Indie Labels into Poor Deals," *The Guardian*, June 3, 2014, sec. Technology, http://www.theguardian.com/technology/2014/jun/04/youtube-independent-record-label-deals; Stuart Dredge and Dominic Rushe, "YouTube to Block Indie Labels Who Don't Sign up to New Music Service," *The Guardian*, June 17, 2014, sec. Technology, http://www.theguardian.com/technology/2014/jun/17/youtube-indie-labels-music-subscription; Amir Efrati, "Reappearing on YouTube: Illegal Movie Uploads," *Wall Street Journal*, February 8, 2013, sec. Tech, http://online.wsj.com/news/articles/SB10001424127887324906004578290321884631206?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424127887324906004578290321884631206.html.

[292] McKay, "Victory! YouTube Reforms Content ID Dispute Process"; Borough, Benjamin, "The next Great YouTube: Improving ContentID," n.d.; "YouTube Announces Improved ContentID Program (Finally)," accessed June 11, 2014, http://newmediarockstars.com/2012/10/youtube-announces-improved-contentid-program-finally/; "Official Blog: Improving Content ID," accessed May 11, 2014, http://youtube-global.blogspot.com/2012/10/improving-content-id.html; "When We Launched Google+ over Three Years Ago, We Had a Lot of Restrictions On…," accessed July 15, 2014, https://plus.google.com/u/0/+googleplus/posts/V5XkYQYYJqy.

[293] "After Heavy Threats, SoundCloud Agrees to Label Licensing Talks..."

[294] "Searching for the Right Balance," *Official Google Blog*, accessed July 14, 2014, http://googleblog.blogspot.com/2014/07/searching-for-right-balance.html.

[295] "YouTube Finally Admits It Totally Screwed Up Rolling Out ContentID To Multi-Channel Networks; Trying To Improve Tools | Techdirt," *Techdirt.*, March 27, 2014, https://www.techdirt.com/articles/20140326/08003126688/youtube-finally-admits-it-totally-screwed-up-rolling-out-contentid-to-multi-channel-networks-trying-to-improve-tools.shtml.

[296] "One Single Porn Copyright Troll, Malibu Media, Accounted For Nearly 40% Of All Copyright Lawsuits This Year | Techdirt," *Techdirt.*, accessed July 13, 2014, https://www.techdirt.com/articles/20140517/06552727268/one-single-porn-copyright-troll-malibu-media-accounted-nearly-40-all-copyright-lawsuits-this-year.shtml; Matthew Sag, *Copyright Trolling, An Empirical Study*, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, July 3, 2014), http://papers.ssrn.com/abstract=2404950.

iii. Financial and Economic Innovation

The "monetization" choice that Content ID offers to rights holders is perhaps its most noteworthy feature, and other than errors and false positives, the focus of the most attention surrounding the program. Diverting the ad revenue stream on a video to the rights holders arguably functions like a compulsory licensing regime, or a sort of private copying levy,[297] but one in which there are zero transaction costs from the user's perspective. Even notoriously protective rights holders, such as Disney,[298] have realized that there is more to be gained by tolerating, and even profiting from, the public's "unlicensed" uses of their intellectual property. Nintendo has gone so far as to offer to split its ad revenue with the users who incorporate its content.[299] The "Nintendo Creator Program" debuted recently to mixed reviews.[300] Looking further into the future, some have even speculated that not only do YouTube and other similar streaming platforms represent a new consumption paradigm[301] that will disrupt existing business models, but also that "views" may actually form the basis of new metrics for success.[302] [303] The distribution of advertising revenue[304] associated with consuming content takes the place of selling a "thing," digital or real. The flexibility that Content ID provides, or more cynically, the liminal zones that it creates, means that YouTube and its constituencies have more niches to fill[305] and surplus to exploit.[306] Hollywood may have seen the writing on the wall, and is taking the YouTube platform very seriously.[307] It's hard to believe that it would have done so without

---

[297] See, e.g. Terry fisher, *Promises to Keep*, chapter 9

[298] Andrew Leonard, "How Disney Learned to Stop Worrying and Love Copyright Infringement," accessed July 10, 2014, http://www.salon.com/2014/05/23/how_disney_learned_to_stop_worrying_and_love_copyright_infringement/.

[299] Sam Machkovech, "Nintendo Announces Plan to Share Ad Revenue with YouTube Streamers," *Ars Technica*, May 27, 2014, http://arstechnica.com/gaming/2014/05/nintendo-announces-plan-to-share-ad-revenue-with-youtube-steamers/; "Nintendo's New Affiliate Program Will Split YouTube Ad Revenue with Proactive Users," *Polygon*, accessed July 9, 2014, http://www.polygon.com/2014/5/27/5754560/nintendo-youtube-affiliate-program.

[300] "Nintendo's YouTube Plan Is Already Being Panned By YouTubers," *Kotaku*, accessed January 29, 2015, http://kotaku.com/nintendos-youtube-plan-is-already-being-panned-by-youtu-1682527904.

[301] "Statistics - YouTube," accessed July 11, 2014, https://www.youtube.com/yt/press/statistics.html. ("reaches more adults than any cable network.")

[302] "Audience as the New Currency: YouTube and Its Impact on Hollywood and Social Media - Brian Solis," accessed June 11, 2014, http://www.briansolis.com/2014/01/audience-as-the-new-currency-youtube-and-its-impact-on-hollywood-and-social-media/.

[303] "Spotify Rules," *Lefsetz Letter*, accessed July 10, 2014, http://lefsetz.com/wordpress/index.php/archives/2014/07/03/spotify-rules/; Victor Luckerson, "Spotify and YouTube Are Just Killing Digital Music Sales," *Time*, accessed July 10, 2014, http://business.time.com/2014/01/03/spotify-and-youtube-are-just-killing-digital-music-sales/.

[304] Todd Spangler, "YouTube to Gross $5.6 Billion in Ad Revenue in 2013: Report," *Variety*, December 11, 2013, http://variety.com/2013/digital/news/youtube-to-gross-5-6-billion-in-ad-revenue-in-2013-report-1200944416/; Farber, "All3Media," 3.

[305] KaskadeVerified account, "Yes, so I Will Move Forward with Constructing My Own Portal Where I Can Share What I like When I Like.," microblog, (June 4, 2014), https://twitter.com/kaskade/statuses/474230686778290177.

[306] "Gamasutra: Colin Sullivan's Blog - YouTube's Content ID Is Not About Copyright Law," accessed July 10, 2014, http://www.gamasutra.com/blogs/ColinSullivan/20131214/207038/YouTubes_Content_ID_Is_Not_About_Copyright_Law.php.

[307] "Why Hollywood Is Making It Rain on the YouTube Ecosystem and Why It's Only Beginning," *PandoDaily*, April 7, 2014, http://pando.com/2014/04/07/why-hollywood-is-making-it-rain-on-the-youtube-ecosystem-and-why-its-only-beginning/; Michael Carney On May 2 and 2013, "An inside Look at the First Major Acquisition of a Premium YouTube Channel," *PandoDaily*, May 2, 2013, http://pando.com/2013/05/02/an-inside-look-at-the-first-major-acquisition-of-a-premium-youtube-channel/.

being first convinced by the sheer scale of content, viewers, and dollars available on YouTube that Content ID made possible.

As just one example of such a new niche, YouTube is uniquely poised to effectively curate its massive store of content,[308] a role becoming ever more vital as data grows beyond human capacity to make sense of it.[309]As the U.S. Congress holds a series of hearings on the future of copyright law in 2014, it is reasonable to speculate that future iterations of copyright law may mandate a similar content monitoring and revenue sharing system, as a way of cutting the current system's Gordian knot.[310] [311] However, from the perspective of start-up businesses and would-be disrupters and innovators, creating or buying a Content ID-like system costs a lot of money, likely far more than having a DMCA-notification procedure in place. The costs associated with such a requirement would effectively raise the barrier to market entry, stifling innovation.

The revenue stream associated with Content ID also represents a new business model for performers and a new, or replacement revenue stream for existing types of artists. Whether the new ways to make money are as lucrative[312] as previous ones is a matter of opinion,[313] but the mere fact that a robust debate as to the viability of the YouTube model exists, and that there are those positioning themselves as guides to the new territory[314] speaks volumes.

5. Negative Outcomes

As will come as no surprise, the most obvious and commonly occurring problem with a vast and impersonal system like Content ID is that it makes mistakes.[315] False positives are probably an unavoidable consequence of any classification system, and are a problem with DMCA notices[316]

---

[308] "Exclusive: 'YouTube Music' Is Launching This Summer...," *Digital Music News*, accessed July 11, 2014, http://www.digitalmusicnews.com/permalink/2014/04/02/youtubesummer; "YouTube Says That 95% of Labels Are Now on Board...," *Digital Music News*, accessed July 11, 2014, http://www.digitalmusicnews.com/permalink/2014/07/01/youtube-says-95-labels-now-board.

[309] Weinberger, David *Too Big To Know;* http://www.hyperorg.com/blogger/2014/05/11/2b2k-in-over-our-heads-my-simmons-commencement-address/

[310] "Google DMCA Takedowns Increase Tenfold, MPAA Still Says Google Not Doing Enough," *Digital Digest*, accessed July 11, 2014, http://www.digital-digest.com/news-63552-Google-DMCA-Takedowns-Increase-Tenfold-MPAA-Still-Says-Google-Not-Doing-Enough.html; Masnick, "MPAA."

[311] "Copyright Hearing Recap: DMCA Notice & Takedown | Future of Music Coalition."

[312] Amanda Holpuch, "Harlem Shake."

[313] "1.2 Million YouTube Views and Not a Penny Earned for Watertown Shootout Video.," June 18, 2013, http://blog.rawporter.com/post/53276959744/1-2-million-youtube-views-and-not-a-penny-earned-for; Zoia, "This Guy Makes Millions Playing Video Games on YouTube"; Lawler, "YouTube Has Found Its Business Model, And Is Paying Out Hundreds Of Millions Of Dollars To Partners"; "I Ain't Gonna Work on YouTube's Farm No More - LAUNCH Blog - LAUNCH Blog," accessed June 9, 2014, http://blog.launch.co/blog/i-aint-gonna-work-on-youtubes-farm-no-more.html.

[314] "How to Make Money on YouTube: 101 Monetization Tips | MonetizePros"; "Making Money on YouTube with Content ID," *Official Google Blog*, August 27, 2008, http://googleblog.blogspot.com/2008/08/making-money-on-youtube-with-content-id.html; 15 and 2013, "AdRev Launches ContentID.com, Brings Music Rights Management to the YouTube Masses."

[315] "Film Distributor, Copyright Enforcement Company Join Forces To Kick Creative Commons-Licensed Film Off YouTube | Techdirt," *Techdirt.*, accessed July 11, 2014, https://www.techdirt.com/articles/20140711/11114227854/us-film-distributor-copyright-enforcement-company-join-forces-to-kick-creative-commons-licensed-film-off-youtube.shtml.

[316] "Google Starts Reporting False DMCA Takedown Requests | TorrentFreak," accessed July 13, 2014, https://torrentfreak.com/google-starts-reporting-false-dmca-takedown-requests-121213/; "Rogues Falsely Claim

as well as with Content ID,[317] but the issue with Content ID is the scale on which it must operate in order to be effective.[318] With one hundred hours of video uploaded to YouTube every *minute*, if even one in a million is incorrectly flagged as infringing, that adds up rapidly.[319]And while some errors may be relatively minor, some can have far-reaching and lasting consequences.[320] Relying on big data and automation means that when errors need human attention to resolve, or to avoid in the first place, problem solving doesn't scale. There's simply no way for YouTube to give human attention to every video, even if that attention is outsourced to rights holders.[321] What percentage of errors is "acceptable" is a difficult – if not impossible – question to answer, especially when some errors are so egregious.[322] The nature of the problem by necessity means that the interest of those actors who operate at scale, whether by volume or wealth, will always be better served, while an individual's will not. YouTube has little incentive (or ability) to tailor Content ID to meet the idiosyncratic needs of a single user, but when that user's videos are affected, the impact on him or her is quite real.[323] The nature of copyright may even mean that the actors the public sees as "responsible" for copyright conflicts may not actually be the ones behind a removal.[324] [325]

Layered on top of the problem with errors is that when user rights are completely defined in the Terms of Service, a user has little recourse, either procedural or substantive, when there is an error.[326] The downside of relying on Content ID instead of the DMCA is that YouTube's Terms of Service and Content ID's internal procedures become de facto law.[327] [328] The First

---

Copyright on YouTube Videos to Hijack Ad Dollars | Threat Level," *WIRED*, November 21, 2011, http://www.wired.com/2011/11/youtube-filter-profiting/all/1.

[317] "YouTube Content ID Under Fire As False Copyright Claims Abound."

[318] "What Is a Content ID Claim? - YouTube Help"; "How Content ID Works - YouTube Help"; "Statistics - YouTube."

[319] "YouTube Copyright Fiasco Get Wilder, But This Time Someone Admits Error," *Kotaku*, accessed June 9, 2014, http://kotaku.com/mistake-zaps-youtubers-with-thousands-of-erroneous-co-1484535253; "YouTube Copyright Chaos Continues. Game Publishers To The Rescue?," *Kotaku*, accessed July 10, 2014, http://kotaku.com/youtube-copyright-chaos-continues-game-publishers-to-t-1481517758.

[320] "Campaign Takedown Troubles."

[321] David Kravets, "Google Says It Won't 'Manually' Review YouTube Vids for Infringement | Threat Level," *WIRED*, October 4, 2012, http://www.wired.com/2012/10/youtube-infringement/; "YouTube Isn't Going to Manually Check Videos for Copyright Infringement after All," *The Verge*, October 4, 2012, http://www.theverge.com/2012/10/4/3457962/youtube-manual-review-content-id; "YouTube's Content ID Disputes Are Judged by the Accuser - Waxy.org."

[322] Singel, "YouTube Flags Democrats' Convention Video on Copyright Grounds | Threat Level."

[323] "Game Critic Says YouTube Copyright Policy Threatens His Livelihood," accessed June 4, 2014, http://www.kotaku.com.au/2013/12/game-critic-says-youtube-copyright-policy-threatens-his-livelihood/; 24th and 2012, "An Open Letter to Jay Leno About Stealing My Video and Then Getting It Removed From YouTube."

[324] Mike Masnick, "Commander Hadfield's Amazing Cover Of David Bowie's Space Oddity Disappears Today, Thanks To Copyright | Techdirt," *Techdirt.*, May 14, 2014, http://www.techdirt.com/articles/20140513/06584027216/commander-hadfields-amazing-cover-david-bowies-space-oddity-disappears-today-thanks-to-copyright.shtml; "YouTube Copyright Chaos Continues. Game Publishers To The Rescue?"

[325] "Blizzard, Capcom, Ubisoft And More Rally Behind Copyright-Afflicted YouTubers," *Forbes*, accessed July 2, 2014, http://www.forbes.com/sites/insertcoin/2013/12/12/blizzard-capcom-ubisoft-and-more-rally-behind-copyright-afflicted-youtubers/.

[326] "YouTube Refuses to Honor DMCA Counter-Notices."

[327] *www.**code-is-law**.org*

[328] "Universal Music Can Delete Any SoundCloud Track Without Oversight | TorrentFreak."

Amendment[329] doesn't apply to YouTube, nor is there any fundamental right to use a private service. Some critics have gone so far as to say that a user's mere knowledge that any uploaded content will be impersonally reviewed will itself have a chilling effect on public discourse.[330]

There is no obvious solution to these problems, at least not one that will please rights holders as well as those afflicted by erroneous takedowns. Solving the false positive issue also requires addressing "correct" content matches that would nevertheless be determined to be a fair use, the Achilles heel of any automatic content review system.[331] Of course, there is no penalty for YouTube if Content ID fails to consider fair use, the way there theoretically is within the DMCA.[332] Finally, with so much power given to YouTube and Content ID, it could easily be said that YouTube is no longer just an intermediary, but a third, equally powerful participant in the relationship between content and consumer, with its own interests at stake, both separate from and intercalated with those of others.

One possible silver lining in this cloud is that the same inability to avoid false positives and the lack of recourse[333] for clear errors by Content ID is incentivizing users to innovate and create their own solutions, including alternative platforms,[334] new types of business organization[335] and revenue sharing[336], and even suggestions for YouTube-centered organized labor.[337] To perhaps stretch the point, Content ID's false positives are acting as a kind of selection pressure on the UGC (video) ecosystem, though it remains to be seen what will survive as "fit."

6. Conclusion

It's likely that as users and rights holders' relationship with YouTube and each other continues to evolve, so will Content ID, as it did following the MCN controversy. A comprehensive private ordering like Content ID, may therefore serve as a "laboratory"[338] for regulation and law with

---

[329] "Online Hitler Parodies Suffer Censorship - FIRST AMENDMENT COALITION," accessed July 13, 2014, http://firstamendmentcoalition.org/2010/04/online-hitler-parodies-suffer-censorship/.
[330] "The YouTube Gaze: Permission to Create? | Enculturation," accessed July 10, 2014, http://www.enculturation.net/the-youtube-gaze.
[331] "How Google's ContentID System Fails At Fair Use & The Public Domain | Techdirt"; "Fair Use Principles for User Generated Video Content," Electronic Frontier Foundation, accessed May 11, 2014, https://www.eff.org/pages/fair-use-principles-user-generated-video-content; "MPAA Freaks Out: Insists That Having To Consider Fair Use Before Filing A DMCA Takedown Would Be Crazy | Techdirt," Techdirt., accessed June 2, 2014, http://www.techdirt.com/articles/20130511/03220823047/mpaa-freaks-out-insists-that-having-to-consider-fair-use-before-filing-dmca-takedown-would-be-crazy.shtml.; http://www.traverselegal.com/copyright-infringement/copyright/how-much-does-it-cost-to-pursue-a-copyright-infringement-claim
[332] http://www.dmlp.org/threats/tuteur-v-crosley-corcoran
[333] "YouTube Copyright Fiasco Get Wilder, But This Time Someone Admits Error."
[334] Miller, "Should YouTubers Launch New Platforms to Compete with YouTube?"; account, "Yes, so I Will Move Forward with Constructing My Own Portal Where I Can Share What I like When I Like."
[335] "Crowdfunding's Patreon Takes Aim At YouTube's Business Model," *Huffington Post*, February 13, 2014, http://www.huffingtonpost.com/turnstyle/crowdfundings-patreon-tak_b_4785138.html; "YouTube Multi-Channel Networks & the Great Music Money Debate," accessed June 11, 2014, http://newmediarockstars.com/2013/03/youtube-multi-channel-networks-the-great-music-money-debate/; Lawler, "YouTube Has Found Its Business Model, And Is Paying Out Hundreds Of Millions Of Dollars To Partners."
[336] Machkovech, "Nintendo Announces Plan to Share Ad Revenue with YouTube Streamers."
[337] "Union For Gamers"; "A YouTube Creators' Bill of Rights (Or 'A Roadmap for Building a Better YouTube') - LAUNCH Blog - LAUNCH Blog," accessed June 9, 2014, http://blog.launch.co/blog/a-youtube-creators-bill-of-rights-or-a-roadmap-for-building.html.
[338] http://scholar.valpo.edu/cgi/viewcontent.cgi?article=1888&context=vulr

respect to liability and may provide templates or cognitive anchors for future legislation. However, more avenues for success mean more possible lines along which to make mistakes. Policy makers will need to recognize that a particular OI's internal schema will, by necessity, suit its own needs, and that a legal or regulatory regime modeled on that of a powerful and successful OI like YouTube will likely favor the existence and survival of similar OIs. Any system will prefer some uses to others, with the inevitable "pruning" and possible chilling effect on innovation along other paths that will result.[339] The dominant players will have again written the rules, but this time indirectly. Ongoing transparency with respect to the way in which private ordering works, as well as paying more than lip service to the public interest, will likely result in both better outcomes and wider acceptance.

[339] Mueller, "Participatory Culture on YouTube: A Case Study of the Multichannel Network Machinima."

C. Private Ordering to Respond to Trademark Concerns – eBay's VERO Program

In the United States, trademarks are words, phrases, symbols, and other indicia used to identify the source or sponsorship of goods or services.[340] Trademark law serves the dual purpose of protecting brand integrity and preventing customer confusion with regard to a product's source or affiliation. Federal trademark law is codified in the Lanham Act, a statute that makes it unlawful to use a valid trademark in a manner that would cause confusion as to the source or sponsorship of goods or services.[341] Ownership of a trademark does not vest upon the mark's creation, and an aspiring trademark owner must actually use their trademark in commerce in connection with goods or services. The Lanham Act also authorizes trademark owners to bring infringement suits to stop or prevent use of a mark by other parties. Unlike other intellectual properties, trademark law is a hybrid of both federal and state law, which complicates the creation and prevalence of concrete standards, particularly issues involving trademark infringement.

Trademark infringement occurs when one party uses another's trademark without permission in commerce, causing confusion at the point of sale or a third party's initial interest. A typical scenario involves the sale of counterfeit goods, or when one party uses the trademark of another in the hopes of free riding off the goodwill created by the trademark owner's investment. Another type of infringement involves false sponsorship or affiliation, where an infringer uses another party's trademark not to mislead consumers as to the source of the product, but rather to attract the goodwill of the borrowed trademark's brand by association with its own product. Initial interest confusion is where an infringer uses another party's trademark, often a competitors', to draw consumers in and ultimately purchase their own product.

Counterfeit goods have always been problematic for brand owners, but the Internet's emergence as a market for goods has made it extremely difficult for trademark owners to bring suit against direct infringers. No longer burdened by international boundaries, and aided by anonymity and the lax registration requirements of online marketplaces, counterfeiters can push counterfeit goods manufactured across the globe into domestic markets with little risk of legal consequences.[342] Finding lawsuits against individual counterfeiters for direct infringement to be both time consuming and financially inefficient, trademark owners began to target online intermediaries under a theory of contributory trademark liability.[343]

Contributory trademark liability is a judicially created legal doctrine rooted in the common law of torts.[344] The seminal case on the subject is *Inwood Labs. Inc. v. Ives Inc.*, where the Supreme Court held that a third party is legally accountable to a trademark owner if it "intentionally

---

[340] http://www.dmlp.org/legal-guide/trademark

[341] Lanham Act, 15 U.S.C. § 1114(1)(a)

[342] National White Collar Crime Center, 2007 Internet Crime Report 5 (2007), http:// www.ic3.gov/media/annualreport/-2007_IC3Report.pdf (""During 2007, Internet auction fraud was by far the most reported offense, comprising 35.7% of referred crime complaints.")

[343] See *Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 984 (9th Cir. 1999),Rescuecom Corp. v. Google Inc.*, 562 F.3d at 124, 131 ; *Playboy Entertainment, Inc. v. Netscape Communications Corp.*, 354 F.3d 1020, 1024 (9th Cir. 2004); *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir. 2010);*Rosetta Stone Ltd. v. Google, Inc.*, 676 F.3d 144, 149 (4th Cir. 2012)

[344] *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 103 (2d Cir. 2010)

induces another to infringe a trademark, or if it continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement."[345] The *Inwood* test initially applied exclusively to manufacturers and distributers of infringing goods, but courts eventually expanded the scope of the doctrine to include Internet service providers (ISPs), which were analogized to flea markets based on their ability to control and monitor the activity of the infringing users.[346] In cases featuring claims against ISPs, judicial analysis has focused on the second part of the *Inwood* test, or the quantum of knowledge necessary to trigger liability.[347]

1. Tiffany v. eBay

In *Tiffany v. eBay*, the Second Circuit attempted to answer the question of whether an online marketplace could be liable for facilitating the infringing conduct of its users.[348] Tiffany, a purveyor of fine jewelry, brought suit against eBay, the leading online auction site, in part for failing to police the site for counterfeit Tiffany products. After identifying eBay's site as a marketplace for goods with sufficient control and monitoring it to be liable under a theory of contributory liability, the court nevertheless determined that generalized knowledge of infringing conduct was not enough to assign liability to eBay based on the infringing actions of its users.[349] The court reasoned that in the absence of specific knowledge of infringing activity, eBay could not be expected to seek out and remove counterfeit listings, and that rights holders were better situated to identify infringing items and bring them to eBay's attention through its Verified Owner's Rights Program (VeRO), discussed below.[350]

The court also considered whether eBay could be liable under a theory of willful blindness, based on its general knowledge of infringing activity. Stating that a service provider may be liable if it has "reason to suspect" that its users are engaging infringing conduct and "looks the other way," the court noted that eBay removed every specific listing brought to its attention and had considerable anti-counterfeit measures in place to combat infringing use.[351] Unfortunately, the court neglected to specify what types of user actions or information would trigger a "reason to suspect" infringing activity. On its face, the language would seem to include general knowledge, which could be a problem for companies with many employees under an agency theory of liability. For example, it is not clear whether liability would attach if an eBay employee received notice of a specific infringing auction and failed to take action, and the court's willful blindness standard may become a battleground for litigation in future actions until some clarification is provided.

2. Moving Forward

The *Tiffany* holding seems to balance the parties' competing interests while distributing burdens according to relative expertise and resources. Encumbering eBay with the legal responsibility to police its site for infringing auctions would have forced it to completely change its operating model, while relieving it from all responsibility would have encouraged it to facilitate even more

---

[345] *Inwood Labs., Inc. v. Ives Labs., Inc.,* 456 U.S. 844, 102 S. Ct. 2182, 72 L. Ed. 2d 606 (1982)
[346] See *Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 984 (9th Cir. 1999)*
[347] *Tiffany (NJ) Inc. v. eBay, Inc.*, 576 F. Supp. 2d 463, 469 (S.D.N.Y. 2008) aff'd in part, rev'd in part, 600 F.3d 93 (2d Cir. 2010)
[348] *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 103 (2d Cir. 2010)
[349] *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 107 (2d Cir. 2010)
[350] See *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 107 (2d Cir. 2010)
[351] *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 110 (2d Cir. 2010)

counterfeit auctions. By placing the initial burden of notice on rights holders, the court authorized eBay's existing model and supported VeRO as a self-policing tool that would allow them to combat counterfeit sales. A rights holder presumably possesses expertise in identifying its own products and trademarks, so owners are presumably better situated than market intermediaries to determine whether an auction contains infringing items. But as the administrator and facilitator of the auction platform, eBay is uniquely situated to remove the identified infringement, and thus assumes the burden of action after sufficient notice of infringing conduct.

While the court moored its decision in the distinction between general and specific knowledge, the opinion was distinctly flavored by eBay's heavy investment in anti-counterfeiting measures. During the relevant period, eBay was spending around $20 million per year on counterfeit prevention initiatives, including a buyer protection program and a fraud engine that automatically searches for counterfeit auctions.[352] Additionally, the court was satisfied that eBay had removed every listing flagged by Tiffany as potentially infringing.

3. The VeRO Program

For online intermediaries facilitating user-to-user sales, the *Tiffany* court's acceptance of eBay's VeRO program is perhaps more instructive than its decision to absolve eBay of any legal obligation to actively monitor its site for infringing content. Generally, VeRO is a self-policing mechanism that places the initial burden of identifying infringing auctions on the holders of intellectual property rights.[353] Under the VeRO program, a rights holder alleging infringement must download and submit a Notice of Claimed Infringement (NoCI) to one of eBay's designated agents. In addition to swearing ownership and a good faith belief that the identified listing actually infringes its rights, the owner must associate the alleged infringement with one of twelve reason codes, which correspond to different types of intellectual property claims.[354] After receipt of a NoCI, eBay removes the identified listings within 24 hours, and often much sooner.[355] EBay then provides the seller with the e-mail address of the accusing rights holder, and the burden shifts to the seller to prove that its auction was legitimate. To reinstate the item flagged for trademark infringement, eBay must receive permission from the filer of the NoCI.

4. History of VeRO

EBay designed VeRO in the wake of the Digital Millennium Copyright Act (DMCA), which established a safe harbor for Internet service providers with copyright infringing users. Under the DMCA, ISPs could avoid liability by removing infringing content after being notified of its existence.[356] Similar to the DMCA, VeRO places the burden of policing eBay's site for trademark infringement on rights holders, who must submit a NoCI to eBay each time an infringing auction is identified. Again mirroring the DMCA, the burden of action shifts to eBay only after notice of specific instances of user infringement. But unlike the DMCA, there is no legally supported recourse for sellers whose auctions are taken down at the request of rights

---

[352] *Tiffany (NJ) Inc. v. eBay, Inc.*, 576 F. Supp. 2d 463, 476 (S.D.N.Y. 2008) aff'd in part, rev'd in part, 600 F.3d 93 (2d Cir. 2010)

[353] http://pages.ebay.com/help/policies/programs-vero-ov.html

[354] "How to report a listing to eBay" http://pages.ebay.com/help/tp/vero-rights-owner.html

[355] *Tiffany (NJ) Inc. v. eBay, Inc.*, 576 F. Supp. 2d 463, 478 (S.D.N.Y. 2008) aff'd in part, rev'd in part, 600 F.3d 93 (2d Cir. 2010)

[356] http://www.dmlp.org/legal-guide/copyright-claims-based-user-content

holders, and eBay conducts no independent investigation into the validity of ownership claimed in a NoCI. Accused sellers are simply provided with the information of the accusing rights holder and asked to contact them directly to resolve any disputes. Consequently, rights holders have every incentive to overzealously send NoCIs, and many auctions for authentic goods are removed and the accounts of individual sellers are wrongly suspended or removed completely.[357]

While serving as eBay's shield, the VeRO program functions as a sword for brand owners interested in curbing legitimate sales protected by the first sale doctrine and nominative fair use. Companies like Tiffany and Louie Vuitton would love the ability to regulate or eliminate legitimate secondary markets for their products, and part of Tiffany's inspiration for bringing claims was eBay's refusal to prohibit the sale of *all* Tiffany items on its site. But the law gives them no right to regulate these markets, and in many ways the VeRO program sacrifices the rights of its users to allow eBay to escape liability. Ultimately, judicial acceptance of VeRO does not provide any new legal authority to mitigate legitimate sales, but it does act as a powerful extralegal tool for rights holders with the desire and wherewithal to regulate a vast secondary market for their products.

5. Outcomes

The Second Circuit's opinion was favorable to online auction sites, but may have been too fact-specific for general application beyond eBay's specific business model. Ultimately, the opinion failed to delineate a clear standard for secondary liability claims against online intermediaries generally, and other online intermediaries wondering whether their own practices are legally sufficient must proceed without clearly demarcated boundaries. Regardless, there are a few facts that seemed particularly persuasive to the court's decision, and similarly situated intermediaries hoping to avoid trademark infringement liability can look to the case for at least some direction for avoiding liability.

First, in light of *Tiffany*, it is fairly reasonable to assume that a notice and takedown system similar to the VeRO program is persuasive, so long as care is taken to actually remove identified listings after receipt of notice. The court made repeated references to eBay's prompt compliance with infringement notices, and similar diligence would seem to greatly increase the likelihood of avoiding trademark liability. Indeed, other online marketplaces have adapted in the wake of *Tiffany*, and Amazon currently utilizes a notice and takedown mechanism very similar to the VeRO program. The familiar looking "rights holder notification" even requires the same assurance of good faith as to rights holders' identities and infringing activity.[358]

Uncertainty remains however, as eBay had several counterfeit initiatives cited by the court, making it difficult to determine whether a VeRO-like program is sufficient, necessary, or simply persuasive. For example, it is unclear whether an online marketplace must also utilize an internal infringement filter akin to eBay's Fraud Engine, whether users accused of infringement must be suspended or removed in certain circumstances, or if simply removing the listing is sufficient. The court also highlighted eBay's consistent steps to "improve its technology and develop anti-fraudulent measures as such measures became technologically feasible and reasonably available," which may suggest that online marketplaces are expected to continually upgrade their

[357] Tiffany (NJ) Inc. v. eBay, Inc., 576 F. Supp. 2d 463, 479 (S.D.N.Y. 2008) aff'd in part, rev'd in part, 600 F.3d 93 (2d Cir. 2010)
[358] https://www.amazon.com/gp/help/reports/infringement

protective measures as new technology becomes feasible.[359] Also, while the sum of eBay's practices were deemed sufficient, the court gave no indication as to whether those practices represent the bare minimum or exceed the legal requirements of an online auction site with trademark infringing users.

Since the holding, *Tiffany* has been cited in over 100 cases, but rarely for cases concerning liability for online intermediaries. In *Rosetta Stone v. Google*, a district court found Google's anti-infringement efforts sufficiently similar to eBay's and absolved Google of any contributory liability on the basis of *Tiffany*.[360] But the Fourth Circuit overturned the decision, holding that *Tiffany* did not apply to Rosetta Stone's claims on Google's motion for summary judgment.[361] The case subsequently settled out of court, leaving an open question of whether Google's AdWords policy amounted to trademark infringement. Additionally, the decision would seem to preclude any reliance on *Tiffany* in a motion for summary judgment, limiting any application of its holding to fact-specific inquiries before fact is tried.

In *1-800 Contacts Inc. v. Lens.com*, the 10th Circuit advocated a stricter standard for online intermediaries providing service to trademark infringing users.[362] Specifically, the court held that nothing in *Tiffany* prevents contributory liability from attaching where the service provider did not *need* specific knowledge of the infringing users identity to prevent the illegal conduct. The court reasoned that "when modern technology enables one to communicate easily and effectively with an infringer without knowing the infringers specific identity, there is no reason for a rigid line requiring knowledge of that identity…"[363] This logic tracks the implicit understanding in *Tiffany* that online marketplaces are expected to update their anti-infringing initiatives alongside technology, which effectively creates a fluid and unknowable standard for contributory trademark liability. Additionally, whether a service provider with general knowledge could have utilized technology to prevent counterfeit infringement would appear to be a question of fact, and widespread adoption of the 10th Circuit interpretation could lead to considerable litigation as identity screening mechanisms become more sophisticated.

[359] *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 100 (2d Cir. 2010)
[360] *Rosetta Stone Ltd. v. Google Inc.*, 732 F. Supp. 2d 628 (E.D. Va. 2010) aff'd, 676 F.3d 144 (4th Cir. 2012)
[361] *Rosetta Stone Ltd. v. Google, Inc.,* 676 F.3d 144, 165 (4th Cir. 2012)
[362] *1-800 Contacts, Inc. v. Lens.com, Inc.,* 722 F.3d 1229, 1254 (10th Cir. 2013)
[363] Id.

D. The State as Soft Power – The Intermediaries Around Wikileaks

1. Introduction

The mission of WikiLeaks.org, which launched on October 4, 2006, is to anonymously publish otherwise private or censored documents in order to promote government and corporate transparency across the world.[364] Led by its editor-in-chief Julian Assange, an Australian computer programmer, publisher, and journalist, and largely relying on anonymous sources, WikiLeaks has subsequently been responsible for publicizing several very large leaks of confidential government information.[365] These leaks made WikiLeaks, its employees, and its sources the target of possible criminal liability.[366] But the online intermediaries that provided services, hosted, or supported WikiLeaks also incurred many risks. Although not faced with direct criminal charges, intermediary supporters of WikiLeaks have been forced to confront government pressures and the potential that legal action could be taken against them. Without much guidance from courts or prior business experiences, online intermediaries responded in various ways to these pressures. This analysis of the WikiLeaks case will examine how online intermediaries responded in the wake of WikiLeaks' dissemination of controversial documents, the United States government's effect on those responses, and what this case means for the future of online intermediaries.

2. Background

Beginning in 2007, WikiLeaks made headlines in the United States by independently releasing numerous confidential documents. These leaks included the Standard Operating Procedures of the Guantanamo Bay Prison, reports on Scientology, U.S. military rules of engagement in Iraq, emails from then-Governor of Alaska Sarah Palin, and, most controversially, a video showing two Apache attack helicopters killing two Reuters employees in Iraq.[367] After WikiLeaks released the Iraq video, the United States arrested and charged U.S. army intelligence analyst Chelsea Manning for obtaining and leaking confidential national security information to WikiLeaks in violation of the Uniform Code of Military Justice, which includes the Espionage Act and the Computer Fraud and Abuse Act.[368] The United States later convicted Manning of 20 offenses and sentenced her to 35 years in prison.[369]

After Manning's arrest, WikiLeaks worked with more established media outlets, such as The New York Times, The Guardian, and Der Spiegel, to release Afghanistan War Diaries and Iraq

---

[364] *About: What is Wikileaks?*, (June 27, 2014, 12:45 PM), https://wikileaks.org/About.html.
[365] Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311 (2011).
[366] *Id.* at 313.
[367] *Id.* at 316–26.
[368] *WikiLeaks: Bradley Manning Faces 22 New Charges*, CBS NEWS, (June 27, 2014, 12:58 PM), http://www.cbsnews.com/news/wikileaks-bradley-manning-faces-22-new-charges/.
[369] Charlie Savage & Emmarie Huetteman, *Manning Sentenced to 35 Years for a Pivotal Leak of U.S. Files*, THE NEW YORK TIMES, Aug. 21, 2013, *available at* http://www.nytimes.com/2013/08/22/us/manning-sentenced-for-leaking-government-secrets.html?pagewanted=all&_r=0.

War Logs in 2010.[370] Then, on November 28, 2010, WikiLeaks and its media partners released 220 United States Embassy Cables to the public.[371] The leaking of thousands of cables, dubbed "Cablegate," contained confidential internal communications between the U.S. government and various embassies from 1966 to 2010.[372] Although WikiLeaks' previous releases had earned worldwide attention, Cablegate nevertheless set off unprecedented scrutiny from the public and the government.[373]

After WikiLeaks released the Cablegate memos, the White House immediately issued a statement, stating that "[b]y releasing stolen and classified documents, WikiLeaks has put at risk not only the cause of human rights but also the lives and work of these individuals."[374] Three days later, on December 1, 2010, United States Senator Joe Lieberman, Chairman of the Senate Committee on Homeland Security, released a statement asking the intermediaries supporting WikiLeaks to end their relationship with WikiLeaks. In Lieberman's statement, he stated, "I call on any other company or organization that is hosting Wikileaks to immediately terminate its relationship with them. . . No responsible company – whether American or foreign – should assist Wikileaks in its efforts to disseminate these stolen materials."[375] Lieberman's staff members also called Amazon to inquire about its hosting of WikiLeaks and the confidential documents.[376]

3. Legal Liability

At the time of the Cablegate releases, WikiLeaks used various intermediary companies to help it maintain its online presence and financial viability. Amazon hosted WikiLeaks.org on its cloud hosting services, while EveryDNS provided the domain name service. WikiLeaks solicited donations through its website using payment processing services such as PayPal, MasterCard, Visa, and Bank of America. Citizens could also access WikiLeaks content through its many social media platforms and other websites and applications that linked to WikiLeaks material.

In general, these online intermediaries would have legal immunity from most liability under Section 230 of the Communications Decency Act (CDA),[377] but Section 230 of the CDA does not apply to federal criminal law.[378] Therefore, online intermediaries such as Amazon, EveryDNS, Twitter, and PayPal could have potentially been liable under federal statutes, including the Espionage Act[379] and laws against material support for terrorism[380] or treason.[381]

---

[370] *See* Benkler, *supra* note 2, at 323–325.
[371] *Id.* at 326–329.
[372] *Id.*
[373] *Id.*
[374] Jennifer K. Elsea, *Criminal Prohibitions on the Publication of Classified Defense Information*, CONGRESSIONAL RESEARCH SERVICE, Sept. 9, 2013, *available at* http://fas.org/sgp/crs/secrecy/R41404.pdf.
[375] *See* Benkler, *supra* note 2, at 339.
[376] Julie Adler, *The Public's Burden in a Digital Age: Pressures on Intermediaries and the Privatization of Internet Censorship*, 20 J.L. & POL'Y 231, 239 (2011).
[377] *See* 47 U.S.C. §§ 230(c)(1) (1996). "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."
[378] *See* 47 U.S.C. §§ 230(e)(1) (1996).
[379] *See* 18 U.S.C. §§ 37.
[380] *See* 18 U.S.C. §§ 2339(A), (B). *See also* Charles Doyle, *Terrorist Material Support: An Overview of 18 U.S.C. 2339A and 2339B*, CONGRESSIONAL RESEARCH SERVICE, July 19, 210, *available at* http://fas.org/sgp/crs/natsec/R41333.pdf.

Although the United States convened a grand jury to consider possible charges against WikiLeaks and Assange,[382] the United States Department of Justice has not taken any formal action against WikiLeaks, Assange, or any third party or business associated with the website.[383] In general, the United States has never prosecuted a journalist or an online intermediary for publishing classified information.[384] In the WikiLeaks case, the United States only brought charges under the Espionage Act against Manning, the source of the illegally obtained documents.[385] But the vague language of the Espionage Act leaves open the possibility of charging non-government employees such as journalists, media outlets, and intermediaries.[386] It is difficult to determine exactly who could be found liable under the Espionage Act.[387] Even though the threat looms, the United States continues to suggest it does not plan to charge a publisher or intermediary in connection to WikiLeaks. A legislative attorney wrote that "There may be First Amendment implications that would make such a prosecution difficult, not to mention political ramifications based on concerns about government censorship."[388]

Those First Amendment implications stem from extensive United States Supreme Court jurisprudence, mostly notably *New York Times Co. v. United States*,[389] also known as the "Pentagon Papers" case, in 1971 and *Bartnicki v. Vopper*[390] in 2001. In the "Pentagon Papers" case, the United States Supreme Court held that under the First Amendment government actions to prevent publication, known as prior restraints, receive the most stringent judicial scrutiny and would only be allowed in extremely rare situations.[391] In *Bartnicki*, the Court extended a principle from the 1979 case of *Smith v. Daily Mail Publishing Co.*[392] and established that publishing truthful information about a matter of public concern, even if obtained through the

---

[381] *See* 18 U.S.C. §§ 2381.
[382] See Ed Pilkington, *WikiLeaks: US Opens Grand Jury Hearing*, THE GUARDIAN, (May 11, 2011), http://www.theguardian.com/media/2011/may/11/us-opens-wikileaks-grand-jury-hearing.
[383] *See* Elsea, *supra* note 11, at 16
[384] *See* Geoffrey R. Stone, *Government Secrecy vs. Freedom of the Press*, 1 HARV. L. & POL'Y REV. 185, 197, 204 (2007).
[385] Among other charges, the United States convicted Manning of 18 U.S.C. §§ 793(e) of the Espionage Act, which states that:
"[w]hoever having unauthorized possession of, access to, or control *over* any document . . . or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits . . . to any person not entitled to receive it . . . Shall be fined under this title or imprisoned not more than ten years, or both."
[386] *See* Stone, *supra* note 21.
[387] *See* Emily Peterson, *WikiLeaks and the Espionage Act of 1917: Can Congress Make It a Crime for Journalists to Publish Classified Information?*, THE NEW MEDIA AND THE LAW VOL. 35 NO. 3, Summer 2011, *available at* http://www.rcfp.org/browse-media-law-resources/news-media-law/wikileaks-and-espionage-act-1917. Steven Aftergood, director of the Project on Government Secrecy for the Federation of American Scientists, said "The Espionage Act is so vague and poorly defined in its terms, that it's hard to say exactly what it does and does not cover." *Id.*
[388] *See* Elsea, *supra* note 11, at 16.
[389] New York Times Co. v. United States, 403 U.S. 713 (1971). The United States filed an injunction against The New York Times, demanding the newspaper stop publishing the Pentagon Papers that detailed military operations and secret diplomatic negotiations of the Vietnam War obtained through an employee of the Defense Department.
[390] Bartnicki v. Vopper, 532 U.S. 514 (2001). *Bartnicki* involved punishment of a radio station after it published an audio recording in violation of the Electronic Communications Privacy Act.
[391] *New York Times Co*., 403 U.S. at 714.
[392] Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 104 (1979).

illegal activity of a third party, is constitutionally protected unless the government's restriction on the speech satisfies a "state interest of the highest order."[393]

Since the relevant documents are truthful, newsworthy, and the intermediaries are not connected to their illegal obtainment, applying the "Pentagon Papers" case and *Bartnicki* to WikiLeaks, means that the only chance an online intermediary would be held liable and not protected by the First Amendment would be if a Court determined there was a high likelihood that the content released through WikiLeaks would bring immediate and grave harm to the country.[394]

4. Online Intermediaries React

It was easy for WikiLeaks to initiate relationships with online intermediaries as the website was still developing and relatively uncontroversial, but as soon as governmental attention and pressures began to mount, the intermediaries quickly began disassociating themselves from WikiLeaks. Many of the intermediaries decided to end their relationship with WikiLeaks even though they had clear First Amendment protection.

On December 1, 2010, three days after WikiLeaks published the embassy cables, Amazon removed WikiLeaks.org from its cloud hosting services, citing violations of its terms of service and that the content on WikiLeaks was potentially damaging.[395] After Amazon's decision, WikiLeaks began using servers in Sweden and France. Two days later, the French company OVH, which was hosting WikiLeaks, went offline after pressure from French Industry Minister Eric Bresson.[396] The Pirate Party in Sweden then became WikiLeaks' sole hosting service.[397]

EveryDNS, which provided domain name service to WikiLeaks, also denied service to WikiLeaks, claiming WikiLeaks received distributed-denial-of-service (DDoS) attacks that affected other EveryDNS clients.[398] For a period of time, Internet users who typed "www.wikileaks.org" into their URL would not be directed to the website. Some users resorted to typing the IP address of WikiLeaks in order to directly connect to the website.[399] WikiLeaks quickly switched to a domain name service in Switzerland and could be temporarily found via "www.wikileaks.ch."[400]

PayPal, an online payment service through which the public could financially support WikiLeaks, suspended its service to WikiLeaks on December 4, 2010.[401] This decision came after the U.S. State Department legal adviser Harold Koh wrote a letter to WikiLeaks stating the

---

[393] *Bartnicki*, 532 U.S. at 534.
[394] *See* Stone, *supra* note 21, at 202. Historical examples of content that would likely bring immediate and grave danger to the nation were "the sailing dates of transports" or "locations of troops" in wartime. *Id.* Stone points out that the content would likely have to instantly endanger American lives and not meaningfully contribute to public debate. *Id.* at 203. "[T]he reason for protecting the publication of the Pentagon Papers was not only that the disclosure would not 'surely result in direct, immediate, and irreparable damage' to the nation, but also that the Pentagon Papers made a meaningful contribution to informed public debate." *Id.*
[395] *See* Benkler, *supra* note 2, at 339.
[396] *Id.* at 340.
[397] *Id.*
[398] *Id.*
[399] *Id.*
[400] *Id.*
[401] *Id.* at 341.

website was engaging in illegal activity.[402] In a statement, PayPal said that it suspended the WikiLeaks account because "our payment service cannot be used for any activities that encourage, promote, facilitate or instruct others to engage in illegal activity."[403] Soon after, MasterCard, Visa, and Bank of America announced they would no longer allow WikiLeaks to accept process payments using their products.[404] This resulted in a 95 percent decrease of donations to WikiLeaks even though the website found some limited funding through other third parties.[405]

Later, in December 2010, Apple removed an iPhone application that allowed users to access WikiLeaks documents.[406] Even though the developer of the app had no direct ties to WikiLeaks, Apple said it removed the app because the app did not comply with local laws and could put people in harm's way.[407]

Although Amazon, EveryDNS, PayPal, and Apple seemed to make their decisions after soft, indirect government pressures, Twitter, another online intermediary, felt direct pressure from United States courts. On December 14, 2010, the U.S. Department of Justice subpoenaed Twitter for WikiLeaks' account information.[408] The subpoena, which came with a gag order, requested the user names, addresses, telephone numbers, bank account details, and credit card numbers of five WikiLeaks leaders associated with WikiLeaks' Twitter account.[409] The subpoena also sought the email addresses and IP addresses for any communications stored on those accounts, which included identifying information of some of the more than 600,000 followers of WikiLeaks' Twitter page.[410] Twitter successfully appealed the gag order in order to disclose the subpoena to its users, but on November 11, 2011, a U.S. federal judge upheld the subpoena under the Stored Communications Act.[411] Although Twitter was the only social media outlet to publicly contest the subpoenas and gag orders, WikiLeaks claims that similar subpoenas have been issued to Google and Facebook.[412]

5. Analysis

Some of the intermediaries publically cited violations of Terms of Use or other contractual violations as why they ended their relationship with WikiLeaks, but pressure from the United States government and threats of criminal liability undoubtedly played a large role.[413] Questions

---

[402] *Id.* at 340.
[403] Jonathan Haynes, *PayPal Freezes WikiLeaks Account*, THE GUARDIAN, Dec. 4, 2010, http://www.theguardian.com/media/2010/dec/04/paypal-shuts-down-wikileaks-account.
[404] *See* Benkler, *supra* note 2, at 340.
[405] Mia Shanley, *WikiLeaks Claims Victory as Credit Card Donations Flow Again*, REUTERS, July 3, 2013, http://www.reuters.com/article/2013/07/03/us-iceland-wikileaks-idUSBRE96214720130703.
[406] Miguel Helft, *Why Apple Removed a WikiLeaks App from Its Store*, THE NEW YORK TIMES, (Dec. 21, 2010 12:29 PM), http://bits.blogs.nytimes.com/2010/12/21/why-apple-removed-wikileaks-app-from-its-store/?_php=true&_type=blogs&_r=0.
[407] *Id.*
[408] Scott Shane & John F. Burns, *U.S. Subpoenas Twitter Over WikiLeaks Supporters*, THE NEW YORK TIMES, Jan. 8, 2011, *available at* http://www.nytimes.com/2011/01/09/world/09wiki.html?pagewanted=all.
[409] *Id.*
[410] *Id.*
[411] Zack Whittaker, *U.S. Judge Upholds Twitter Subpoena of WikiLeaks' Followers*, ZDNET, (Nov. 11, 2011, 1:42 PM), http://www.zdnet.com/blog/london/u-s-judge-upholds-twitter-subpoena-of-wikileaks-followers/842.
[412] Shane & Burns, *supra* note 45.
[413] *See* Benkler, *supra* note 2, at 314.

remain as to what these decisions by the intermediaries tell us about the relationship between the United States government and online intermediaries and what it means for the future of the Internet and free speech.

The WikiLeaks case is an example of how the United States government censored potential Internet content through extralegal means. Although the law did not empower the government to stop the intermediaries from associating with WikiLeaks, the soft power of the government led to the suppression of speech by limiting the means in which the content could reach the public. The government's influence stemmed, for at least the time being, the dissemination of WikiLeaks materials. Just as traditional print media relied on common mail carriers to transmit newspapers, so do modern-day online media outlets rely on online intermediaries for distribution and spreading of their content. Instead of the government, private companies who maintain the Internet's infrastructure are increasingly often the gatekeepers of which messages are allowed to freely flow online.[414] If the United States government, through extralegal avenues, is able to control online intermediaries by skirting the limits of the Constitution, the government, in turn, is able to stifle online speech without running afoul of the First Amendment. Although practical considerations are of course a major obstacle, truly guaranteeing free speech online will require an Internet free from of government censorship in conjunction with a robust private infrastructure that supports free speech.[415]

i. What, If Anything, Can be Done?

Since online intermediates are private companies and are not constrained by the limits of the Constitution, they are only governed by the contracts they sign with their customers. As a result, the terms of service controlling online speech end up being stricter than restrictions on public speech. There are limited options for WikiLeaks or other disseminators of online speech to fight against suppression by intermediaries. WikiLeaks could sue the intermediary for wrongful denial of service, arguing there is an implied contractual obligation to not withhold service unreasonably or without good faith.[416] WikiLeaks could also sue the government for tortuous interference with contractual relations, but it would be difficult to prove that government intervention caused the intermediary to break the contract with WikiLeaks.[417]

Without the power of law encouraging intermediaries to keep freedom of expression robust on the Internet, one of the only remaining influences over the intermediaries is the power of the consumer. If public backlash is strong enough, intermediaries may think twice about refusing service to organizations like WikiLeaks. This is difficult because of the layers of secrecy between the government and the intermediaries that restrict disclosures to the public. For example, it was only after Twitter appealed the gag order that the public found out about the subpoenas it received from the government. This earned praise from many organizations and users of the social networking website.[418] The United States government submits more than 50,000 subpoenas each year, known as national security letters, with gag orders that prevent

[414] *See* Adler, *supra* note 13, at 237.
[415] *Id.* at 253.
[416] *See* Benkler, *supra* note 2, at 367.
[417] *Id.* at 367–370.
[418] Ryan Singel, *Twitter's Response to WikiLeaks Subpoena Should Be the Industry Standard*, WIRED, Jan. 11, 2011, *available at* http://www.wired.co.uk/news/archive/2011-01/11/twitter-subpoena-reaction.

revealing to the public what the subpoenas seek or even that the subpoenas exist.[419] These gag orders stifle public debate on the topic of national security letters. If the public does not know what is going on between the intermediaries and the government, the public will not be able to put pressure on intermediaries.

ii. Why Only WikiLeaks?

The WikiLeaks case study also brings up the question of why the intermediaries disassociated themselves from WikiLeaks.org but not the other websites that were distributing the same material. The Cablegate documents that caused the intermediaries to separate themselves from WikiLeaks were not uniquely posted on WikiLeaks.org; they were also available on the websites of The New York Times, The Guardian, and Der Spiegel.[420] Nevertheless, the intermediaries did not change their policies related to the more established press entities. The intermediaries drew a line between the established press and WikiLeaks, a website who claims to be part of the press but is often cast as "rogue" or anti-American.[421] Although the Constitutional protections given to WikiLeaks and the other outlets are largely the same,[422] the decisions by the intermediaries showed a clear difference in policy between the intermediaries and WikiLeaks and the intermediaries and other media outlets.[423] For whatever reason this policy difference exists – possibly due to differences in organizational structure, technology, or the intent of WikiLeaks compared to the established press – this stark difference in treatment puts online ventures, especially ones not conforming to traditional norms or paradigms, e.g. "the press", at a greater risk than traditional media outlets.[424] This disparate treatment undermines the quality of our public disclosure and weakens the important function of the newly developing fourth estate in the networked information society.[425]

iii. What Will the Impact be on Economics, Social Progress, and Innovation?

There are several different downstream consequences of the WikiLeaks case study. After seeing Amazon, EveryDNS, PayPal, and Apple bow to government pressure, online intermediaries faced with similar dilemmas will more easily make the same decision. If and when future online intermediaries are approached with the question of whether to support OIs that are publishing questionable material, especially confidential national security material, an example has already set by some of the most powerful intermediaries in the country. Additionally, the outcome of its efforts with respect to WikiLeaks surely reassures the United States government that pressuring private companies yields successful results, which will only encourage similar pressure in the future. Finally, it may chill the speech of other online speakers who may think twice about voicing their opinion online for fear their speech will be suppressed by the intermediaries.

---

[419] Noam Cohen, *Twitter Shins a Spotlight on Secret F.B.I. Subpoenas*, THE NEW YORK TIMES, Jan. 9, 2011, *available at* http://www.nytimes.com/2011/01/10/business/media/10link.html?partner=rss&emc=rss&_r=0.

[420] *See* Benkler, *supra* note 2, at 326.

[421] *Id.* at 385–396.

[422] *See* Branzburg v. Hayes, 408 U.S. 665 (1972). *See also* Citizens United v. Federal Election Commission, 558 U.S. 310 (2010). "We have consistently rejected the proposition that the institutional press has any constitutional privilege beyond that of other speakers."

[423] *See* Benkler, *supra* note 2, at 358.

[424] *Id.*

[425] *Id.* at 362.

E. Online Intermediaries and Transparency Reporting

1. Introduction

As online intermediaries move beyond simply delivering content to end users and become persistent cloud storage networks for all of a user's communications and online interactions, these intermediaries have become incredible resources for law enforcement and intelligence agencies. This puts online intermediaries in a difficult situation with respect to their users. On the one hand, user trust is a central part of their business model: if users cannot trust these companies, they will not entrust them with sensitive personal material such as photographs, e-mails, texts, and other documents. But on the other hand, companies are legally required to comply with the law of the countries in which they operate. Some of these laws require companies to disclose their users' sensitive data (ranging from metadata to actual content) when presented with a valid legal request such as a warrant, subpoena, or court order.

Many of the world's largest online intermediaries are products of California's Silicon Valley, and are thus US companies bound by US law. When discussing issues such as human rights and online censorship, this location has been considered an asset, often allowing companies to claim immunity from the laws of the countries in which they don't (yet) operate.[426]

US-based intermediaries, however, have never claimed to be immune from US legal jurisdiction. And the revelations of Edward Snowden regarding the NSA have shown how that jurisdiction subjects these companies to the surveillance demands of US intelligence agencies.[427] While the media focus of the past year and a half has been on the depth and breadth of those intelligence demands, these companies are equally subject to the requests of other US law enforcement agencies from the federal level all the way down to the local level.

Regardless of whether the demands are from intelligence agencies or local sheriff's offices, they place the companies in a difficult situation. How do they comply with valid requests while maintaining the critical trust of their users? Over the past year there has been an explosion in the use of transparency reports as one way to navigate this difficult tension. One of the audiences for these reports is the users of the service;[428] for these users, the report symbolizes a commitment to

---

[426] *See* Eva Galperin, *What Does Twitter's Country-by-Country Takedown System Mean for Freedom of Expression?,* EFF (Jan. 27, 2012), https://www.eff.org/deeplinks/2012/01/what-does-twitter's-country-country-takedown-system-mean-freedom-expression ("Like all companies (and all people) Twitter is bound by the laws of the countries in which it operates, which results both in more laws to comply with and also laws that inevitably contradict one another. Twitter could have reduced its need to be the instrument of government censorship by keeping its assets and personnel within the borders of the United States, where legal protections exist like CDA 230 and the DMCA safe harbors (which do require takedowns but also give a path, albeit a lousy one, for republication).").

[427] *See, e.g.*, Timothy B. Lee, *Here's everything we know about PRISM to date*, Washington Post, June 12, 2013, *available at* http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/

[428] Interviews conducted with several companies about their transparency reports have revealed that there are several audiences that companies are often trying to reach through their transparency reports. Other audiences for transparency reports include policy makers, investors, law enforcement agencies, and even employees within the company itself. This series of case studies focuses on the legal obligations (and potential liability) placed upon online intermediaries. In the context of government requests for user data, these obligations most directly affect

openness and offers assurances that the company is not complicit in mass or indiscriminate surveillance. The reports, however, are an incomplete solution. They are subject to misunderstandings and ultimately serve as incomplete proxies for the real issue: the trustworthiness of companies and the extent to which they will go to protect the privacy of their users.

2. Legal Background

The legal requirements for the disclosure of user data are found in several areas. At the federal level, the requirements come from two key sources. The primary authority enabling the federal government to compel companies to surrender customer data in criminal investigations is found in the Stored Communications Act (SCA). By contrast, the authority for intelligence investigations is found primarily in the Foreign Intelligence and Surveillance Act (FISA). The authority used to compel the data disclosure is important for several reasons: it determines the legal standard that must be used, the kind of data that can be collected, and even how companies can write their transparency reports.

Although these authorities are described in greater detail in the legal primer section of this paper,[429] a brief review is useful here. In short, there are three main kinds of legal processes for criminal investigations: subpoenas, court orders (often called d orders because the authority is located in Section 2703(d) of SCA), and warrants. Because subpoenas and d orders are easier to obtain, law enforcement may only use them to collect basic subscriber information and other non-content information. Warrants are more difficult to obtain, requiring convincing a court that there is "probable cause" that information related to a crime is in the specific place to be searched. Because they are harder to obtain, warrants can be used to collect content information, such e-mail subject lines, e-mail content, and instant message text.

There are also three legal processes for intelligence investigations: National Security Letters (NSLs), section 215 of the USA PATRIOT Act, and section 702 of the FISA Amendments Act. NSLs allow the FBI to obtain telephone and e-mail records (and associated billing records), "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities," but not the content of the messages themselves.[430] Section 215 authority allows secret court orders, approved by the Foreign Intelligence Surveillance Court (FISC), requiring third parties, such as ISPs or telephone providers, to provide business records deemed relevant to terrorism or intelligence investigations. The third authority is Section 702 of the FISA Amendments Act, which allows the government to collect both the content and non-content information of targeted non-U.S. persons reasonably believed to be outside of the United States.

Subpoenas, d orders, warrants, 215, and 702 orders represent just some of the wide array of legal tools at the disposal of American law enforcement and intelligence agencies. It is this collection of legal tools that put American-based online intermediaries into a difficult position. There are very few options available for companies that are served valid legal process, other than compliance. Generally speaking, that is for the best – it would undermine civil society and

---

companies who are compelled to disclose data, the users whose data is disclosed, and users whose trust in the company is eroded because of those compelled disclosures. Because of that, this paper focuses most directly on transparency reports as a means of communicating with those users.

[429] *See supra*, pp 16-17

[430] 18 U.S.C. § 2709(b)(2).

respect for law if companies could pick and choose the laws that they comply with. Unfortunately, the invasiveness of these legal demands risks undermining the relationship between the companies and their users.

3. Transparency Reporting: Resolving the Tension Between Compliance and Trust?

One of the key ways that companies have tried to maintain the trust of their users while still complying with valid legal process is through the publication of transparency reports. These reports, which document the amount and type of legal process that law enforcement agencies and government have served on a company, are a relatively new phenomenon. Prior to Edward Snowden's first NSA leak on June 9, 2013, only seven American Internet or telecommunications companies had published transparency reports (LinkedIn, Google, Sonic, Dropbox, SpiderOak, Twitter, and Microsoft). In the year that followed, 18 additional companies released transparency reports. Thus, the revelations about the scope of NSA surveillance – and the attention that those news stories garnered – served to build momentum for transparency reporting.

With this surge in reporting taking place only within the last year, transparency reports are very much an on-going experiment. The 25 current transparency reports represent a vast array of preferences, choices, and techniques for presenting this information. And because they are so new, a clear consensus has not yet developed around them. That being said, there are three important observations we can draw from transparency reports and the companies' attempts to use them to restore and maintain user trust.

4. National Security Data is Complicated

Although the stories of NSA surveillance may have catalyzed the use of transparency reporting, domestic law enforcement data requests are actually the more commonly reported category of data. 18 of the 25 transparency reports include domestic law enforcement requests, and only 15 include data on FISA requests or NSLs. However, more significant than the number of reports is the fact that companies provide far greater *detail* about domestic law enforcement requests than they do for national security requests.

The reason for this disparity in detail between reporting about domestic law enforcement requests and reporting about national security surveillance is due to complex legal restraints. Companies are generally free to publish as much detail as they wish with regards to domestic law enforcement requests. In fact, one company has taken the maximalist approach of publishing a list of every single such report it has received.[431]

By contrast, the government requires companies' reports to be quite circumspect with regards to disclosures about FISA and NSL requests. These restrictions come from a January 27, 2014 agreement between the U.S. Department of Justice and the major Internet companies.[432] This agreement leaves companies with two, and only two, approaches to publishing information about national security related requests. The first option allows companies to report the following categories of data:

- Number of NSLs received

[431] *See* Credo Mobile, 2013 Transparency Report, http://www.credomobile.com/transparency-2013
[432] http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf

- Number of customer accounts affected by NSLs
- Number of FISA orders for content information
- Number of "customer selectors targeted under FISA content orders"
- Number of FISA orders for non-content information
- Number of "customer selectors targeted under FISA non-content orders"

However, all of those categories can only be reported in bands of 1000 starting with 0–999. The second option allows companies to report in bands of 250 starting with 0–249. But companies using this option may only report:

- Number of national security requests received (FISA and NSL together in one number)
- Number of "customer selectors targeted under all national security process"

Because of these restrictions, it has been difficult to extract from transparency reports valuable information relating to national security process. While NSA surveillance may have prompted an explosion in transparency reporting, the reports available say far more about domestic law enforcement than they do about the NSA. That fact, however, does not diminish the value of transparency reports as a way of understanding domestic criminal surveillance. Indeed, one thing that we've learned from transparency reports is that online intermediaries receive just as many requests (if not more) for domestic criminal surveillance than intelligence related surveillance.[433] Thus, although the focus on the NSA may have been misplaced as the motivation for transparency reporting, the end result has provided data helpful for understanding the scale and scope of the surveillance burdens placed upon online intermediaries as a whole.

5. Transparency Reports Describe a Passive Event

The biggest challenge for transparency reports as a tool for reestablishing and maintaining trust between companies and their users is that the data often provides little that explains how companies are trying to protect user data. The reason for this stems from the fact that transparency reports are largely documenting a passive event on the part of companies; transparency reports say more about governments than companies. If a company's transparency report shows a large number of government requests for their user data, that could indicate one of three things:

- The government is aggressively investigating the users of this company
- The company has a large number of users
- The users of this service are more likely to be engaged in criminal activity

Importantly, none of those three possibilities relates to the trustworthiness of the company itself, and that's because companies have no control over the number of requests they receive.

Companies do, however, have control over how they handle those requests. Companies can carefully scrutinize requests to ensure that they are responding only to valid requests. But, once

[433] Ryan Budish, *Tech firms should be allowed to publish more data on US surveillance*, Guardian (July 18, 2013), at http://www.theguardian.com/commentisfree/2013/jul/18/tech-firms-letter-nsa-surveillance-transparency "[I]f our estimates are correct, national security surveillance accounted for only about 13% of the total requests Microsoft received and 54% of the total accounts surveilled. That means that non-secret criminal surveillance of Americans is as pervasive, if not more so, than the secret national security surveillance.").

again, transparency reports are ill suited to document this. If a company's transparency report shows that they have responded to every single government request, it may be because they haven't scrutinized the validity of the requests. But it may also be because every single request was valid, even after careful scrutiny. Thus, transparency reports are often weak proxies for determining company trustworthiness.

6. Companies Are Competing With Transparency Reports

Although there are clearly challenges with transparency reports, many companies are innovating with their reports, both to address some of these weaknesses, and to compete with their peers.

A good example of innovation comes from the user notice section of Tumblr's transparency report.[434] User notice, like the volume of requests received, presents a problem for transparency reports because there may be many reasons why a company may or may not provide notice to a user, making a basic percentage misleading. For example, a company may choose (or be compelled) to not provide notice because the request is sealed or because or because the company concluded on its own that notice might disrupt an investigation. This concern is particularly salient in child pornography investigations, where notice to the suspected user might prompt them to delete evidence. Transparency reports are often too blunt a tool to express these subtleties in company decision-making.

Tumblr has tried to address this deficiency within existing reports by providing detailed data about the percent of notice for each of eight different kinds of legal investigations. For instance, Tumblr's data shows that they provide notice in only 1% of "Harm to Minors" investigations and 0% of suicide investigations. Had Tumblr reported the percent of time they provided user notice cumulatively for all types of investigations, their lack of notice in child pornography cases would have made it appear that Tumblr was providing less notice to users overall. Making the effort to categorize requests by type of investigation is not easy, but it pays dividends by helping users understand more about Tumblr's approach to user notice in different circumstances. No other company is as of yet providing this level of specificity for user notice in their transparency report.

There are other examples of innovation in transparency reporting. For instance, Verizon[435] and AT&T,[436] two of America's biggest cellular service providers, have reported the number of requests for user location information, as well as the number of law enforcement requests for "cell tower dumps" – lists of every single phone number connected to a particular cellular tower. Although the latter is specific to mobile phone service, location data is something many intermediaries track and (presumably) share with law enforcement and intelligence agencies, but it has yet to make it to many other transparency reports.

In conversations with many companies that have released transparency reports, we've learned that companies often look to peer companies' reports for inspiration when creating their own reports, but also seek to outdo existing reports with new levels of detail or innovative features. Thus, more recent transparency reports tend to make standard the features that were more

[434] Tumblr's Transparency Report, at http://transparency.tumblr.com/tagged/providing-user-notice
[435] Verizon Transparency Report: US Data, at http://transparency.verizon.com/us-report?/us-data
[436] AT&T Transparency Report, at http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html

innovative just a year ago. For instance, separating content from non-content requests, identifying emergency requests, and listing subpoenas, court orders, and warrants separately have all become the norm in more recent reports, when they were rarely done a year ago. Because companies seek to outdo each other with their transparency reports, it would not be a surprise to see these innovations spread to other reports, and to see further innovations in reporting that do even more to help users regain trust in online intermediaries.

7. Conclusion

Online intermediaries increasingly find themselves in a difficult situation. How do they maintain the trust of their users while complying with valid legal demands to disclose user data to the government? One approach that has gained traction over the past year has been through transparency reporting. These reports, however, are incomplete proxies for company trustworthiness. This is largely due to the fact that companies have no control over the number of requests they receive and the validity of those requests. Despite this issue, reports, taken as a whole, help us better understand the often secretive and fragmented law enforcement environment that intermediaries operate within.

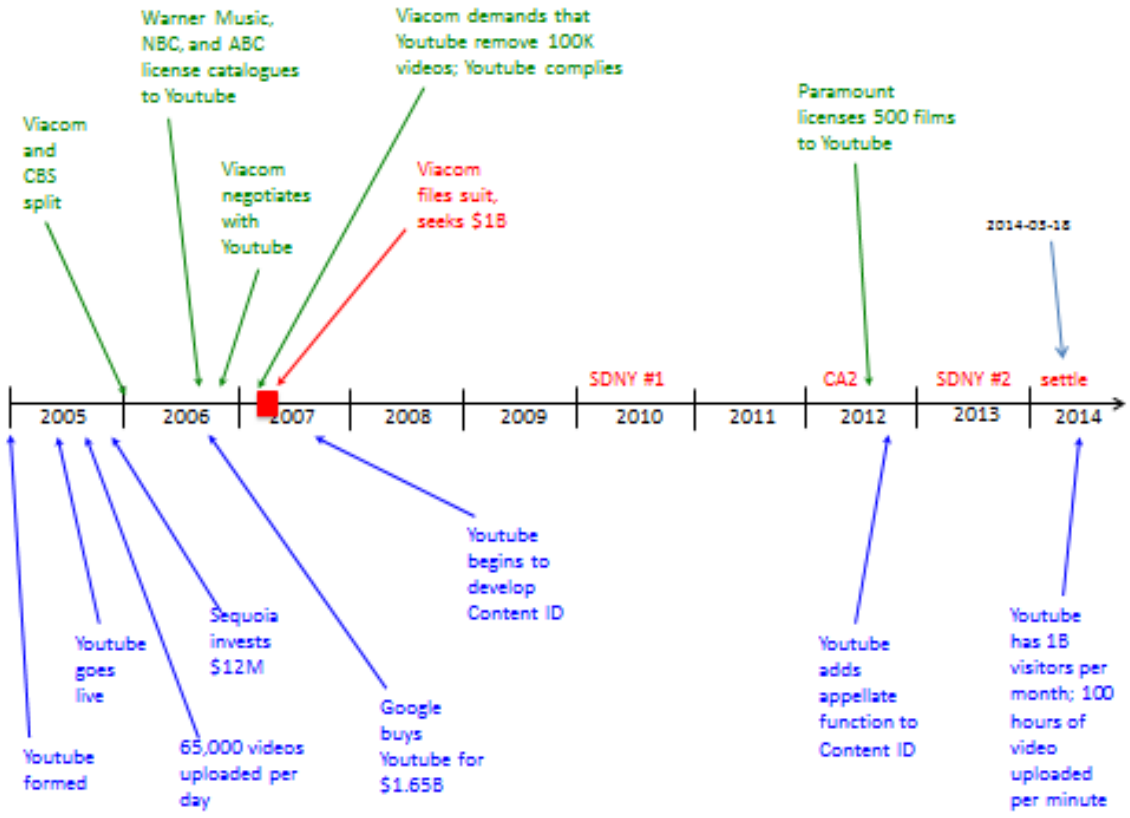
Ultimately, law enforcement requests and surveillance are government issues, not corporate ones. Thus, a government that wanted to enhance user trust for the companies that operate within its legal boundaries might take it upon itself to offer transparency reports of its own. Or better still, it would place significant legal restraints upon its ability to collect user data in the first place. But in the absence of those steps, transparency reports serve a useful role in providing a sense of the scope of law enforcement requests and government surveillance. To the extent that such reports show that only a small percentage of users are impacted by law enforcement requests and surveillance, they are indeed helpful for reestablishing and maintaining user trust. However, transparency reports are primarily statements about government activity, and there is little a transparency report can do to directly change government behavior. Additionally, there have been no studies conducted to identify any impact from transparency reports on either user behavior or corporate bottom lines.[437] However, to the extent that they demonstrate the scope of government data collection, the reports may help contribute to the policy discussion that could have the biggest impact on user trust: a change in government data collection and surveillance behaviors.

[437] We do, however, has evidence that the revelations about NSA surveillance have cost online intermediaries somewhere between $35 and $180 billion dollars in lost business. Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, NY Times, Mar. 21, 2014, at http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html

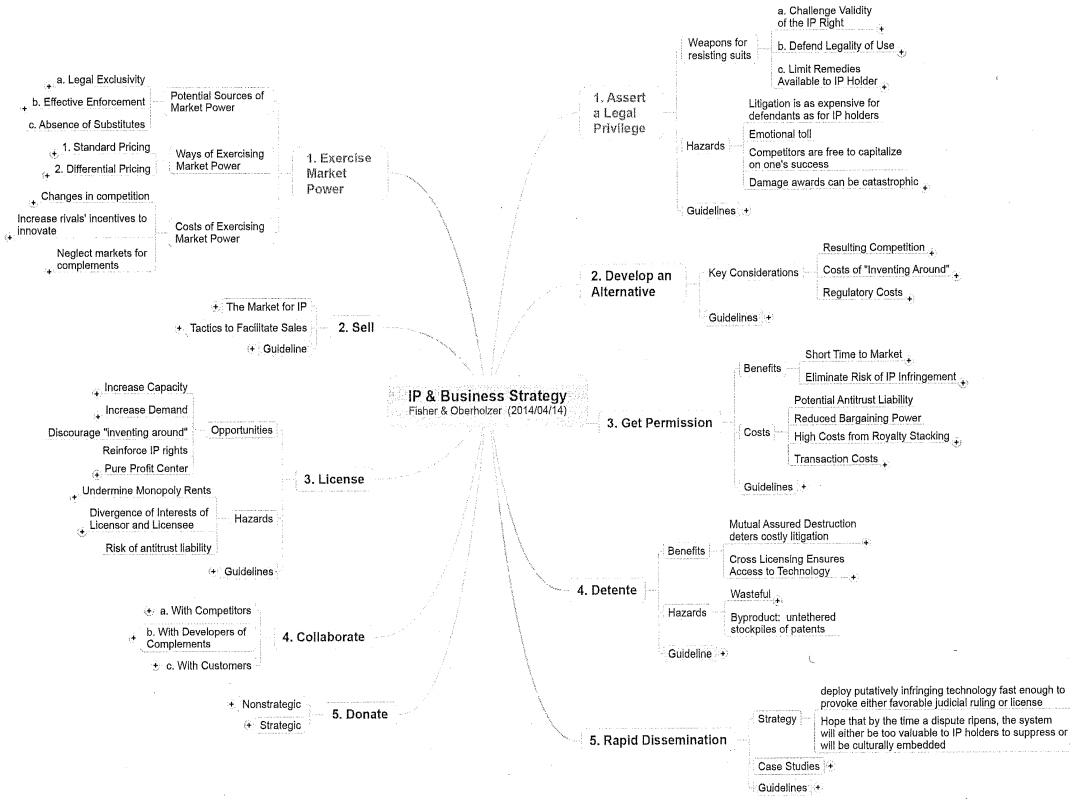
F. Appendix A: Literature Review

The literature review can be found as a living document here: https://docs.google.com/document/d/13iRhW3qTqbMio_QhqSQoPd7fi0Z45iCDC3HFWls0ODg/edit?usp=sharing

G. Appendix B: Youtube and ContentID Timeline



H. Appendix C: Business Strategies Mind-Map



(Fisher & Oberholzer-Gee)

Appendix H:
Roles and Liability of Online Intermediaries in Vietnam – Regulations in the Mixture of Hope and Fear

NoC Online Intermediaries Case Studies Series: Roles and Liabilities of Online Intermediaries in Vietnam – Regulations in the Mixture of Hope and Fear

Thuy Nguyen[1]

Editorial Note: Context, Character, and Purpose of the Case Study

This case study is part of a globally coordinated, independent academic research project by the Global Network of Interdisciplinary Internet & Society Research Centers (NoC). Facilitated by the Berkman Center for Internet & Society at Harvard University, the project is the first output of a larger policy-oriented research initiative that examines the rapidly changing landscape of online intermediary governance at the intersection of law, technology, norms, and markets. In concert with other research projects, it seeks to develop criteria, comparative methods, and a shared data repository, and to compile insights and lessons learned across diverse communities of knowledge aimed at informing and improving Internet policy-making globally.

The initial research output consists of a case study series exploring online intermediary liability frameworks and issues in Brazil, the European Union, India, South Korea, the United States, Thailand, Turkey, and Vietnam, and a synthesis paper that seeks to distill key observations and provide a high-level analysis of some of the structural elements that characterize varying governance frameworks, with a focus on intermediary liability regimes and their evolution.

The authors of these case studies have participated in a multi-step process of in-person consultations and remote collaborations among a global team of researchers from the Network of Centers. Additionally, the case studies are based on a set of broader questions regarding the role of online intermediaries in the digital age.[2]

The research effort is grounded in a diversity of global perspectives and collaborative research techniques, committed to objective and independent academic standards, and aspires to be useful, actionable, and timely for policymakers and stakeholders. More broadly, the Network of Centers seeks to contribute to a more generalized vision and longer-term strategy regarding the role of academic research, facilitation and convening, and education and communication in the Internet age. For additional information on the initiative, please contact Urs Gasser, Berkman Center for Internet & Society, at ugasser@cyber.law.harvard.edu.

---

[1] Thuy Nguyen wrote this chapter when she was an LL.M candidate at Harvard Law School and an intern at the Berkman Center for Internet and Society. *All translations appearing within this essay are considered unofficial and prepared by the author for the ease of the reader's reference, unless otherwise noted.*

[2] The process is documented at: "Online Intermediaries: Functions, Values, and Governance Options", The Global Network of Internet & Society Research Centers, 2014 https://drive.google.com/file/d/0B_ToTBKP5ITVWTl0UzV0U3B2RlU/view?usp=sharing.

Abstract: This essay studies the policy and regulatory framework affecting the liability of online intermediaries in Vietnam. Through this essay, readers will explore how the liability of online intermediaries is shaped by the local authority's ideology, concerns, and hopes, as well as other political and economic factors regarding the information, communications, and technology sector. Maximizing local regulatory sovereignty over all types of Internet activity is the dominant feature of the current Vietnamese policy and regulatory landscape. This happens through various regulatory tools: server localization requirements, compulsory licensing or registration with the local government, required authentication of users' identification, and extensive reporting obligations, among others. At the same time, there is also an image of Vietnam as strongly desiring to grasp the opportunities brought by the online environment in order to boost domestic economic development. This desire is mixed with the protectionist effort, which aims to promote locally branded online goods and services, favor homegrown online intermediaries, and capture domestically a larger portion of the income generated inside Vietnam by foreign businesses. A close look at the Facebook blocking case will illustrate this particular situation. Finally, to complete the picture of the Vietnamese regulatory and policy landscape, this essay also discusses the local regulatory attempts regarding the responsibilities of online intermediaries in protecting national security, data privacy, and network security.

Table of Contents

I. Introduction

Vietnam seems to possess a notorious record regarding its treatment of the Internet. The organization Reporters without Borders refers to the country as one of the "enemies of the Internet."[3] The Information Technology & Innovation Foundation names Vietnam as the author of one of the "10 worst innovation mercantilist policies of 2013."[4] The country also has a record of suppressing online dissidents.[5] However, there is also another Vietnam that is less known internationally − one with the ambition of becoming an information economy, with information technology as the "focal industry" for economic growth. Recent legal and policy developments regarding online intermediaries in Vietnam reflect both of these images.

This essay focuses on analyzing the fears and hopes related to online activities, and the corresponding policies and regulations by the Vietnamese authorities. Relevant cases, regulations, and draft regulations will be analyzed to illustrate the roles and liabilities of online intermediaries.

Online activities bring both hope and fear to the current regime. Since the early 1990s, fear of the Internet as an untested technology that might affect the integrity of the current regime has led to regulations that allow the Vietnamese authorities to exercise heavy censorship and maximum controlling power over online activities. One of the regulatory tools used then was requiring all entities wishing to connect to the Internet to locate their servers in Vietnam and to connect to the Internet through a limited number of government-licensed international gateways. Furthermore, setting limits for what was admissible online content and what had to be be removed was crucial for maintaining the current regime. This control was deemed particularly important in the context that online platforms could be used to easily gather or organize anti-government forces. This set of fears resulted in heavy burdens for online intermediaries. For instance, in order to fully control local online activities, the government recently required online social network service suppliers to ensure that their users supply accurate personal information. Related, a national online identification database, which is under construction, will be used to verify personal information of online social network users.

---

[3] See Reporters without Borders, Enemies of the Internet 2013 Report, March 12, 2013, available at http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-Internet_2013.pdf, accessed on February 28, 2014.

[4] See Michelle A. Wein and Stephen J. Ezell, The 10 Worst Innovation Mercantilist Policies of 2013, The Information Technology & Innovation Foundation, January 2014, available at http://www.itif.org/pressrelease/ten-worst-innovation-mercantilist-policies-2013, accessed on February 28, 2014.

[5] See Human Rights Watch, Vietnam: Clinton Should Spotlight Internet Freedom, July 9, 2012, available at http://www.hrw.org/news/2012/07/09/vietnam-clinton-should-spotlight-Internet-freedom, accessed on March 3, 2014; See also Eva Galperin, Free Expression in Danger as Bloggers and Activists Go On Trial in Vietnam, Electronic Frontier Foundation, January 7, 2013, available at https://www.eff.org/deeplinks/2013/01/bloggers-trial-vietnam-are-part-ongoing-crackdown-free-expression, accessed on February 10, 2014; See also Dara Kerr, Vietnam: Criticize Government on Social Media and Go to Jail, CNET, December 12, 2013, available at http://asia.cnet.com/vietnam-criticize-government-on-social-media-and-go-to-jail-62223058.htm, accessed on February 20, 2014; Committee to Protect Journalist, 2013 Prison Census - 211 Journalists Jailed Worldwide, as of December 1, 2013, available at http://www.cpj.org/imprisoned/2013.php, accessed on February 25, 2014.

In conjunction with the increasing popularity of the Internet in the country, Vietnam also gradually enacted regulations to address the traditional fears felt by other nations, including those concerning national security, fraud prevention, data and privacy protection, and network security. Some of the measures put into place in Vietnam are similar to those adopted in some other jurisdictions following the NSA revelation incident. Other measures addressed specific concerns regarding recent online frauds and security risks in Vietnam.

Moreover, the fear of the consequences of inadequate control, and a perceived need to localize the benefits of online services, has recently resulted in regulations and proposed regulations that exhibit a protectionist tendency for the domestic service suppliers, which involves the use of some regulatory tools similar to those used in the 1990s. In particular, some recently adopted regulations require the localization of servers as one of the conditions for the provision of certain online services in Vietnam. The blocking of Facebook, which has been in place since 2009, will be analyzed in detail to reveal its potential protectionist motivations. The essay will also explain how the "Vietnamese people prefer Vietnamese products" campaign affects the liabilities of online intermediaries.

At the same time, Vietnam's government sees the benefits of developing a strong domestic information technology industry, attracting high tech foreign investment, training a tech-savvy generation, boosting e-commerce, enforcing intellectual property protection, creating clear and transparent rules for e-commerce, and using online social networks to promote local businesses. Some major regulations will be analyzed to demonstrate this contrary perspective of the Vietnamese government towards online intermediaries.

Going forward, online intermediaries will likely experience strong opportunities to grow in Vietnam. However, they might have to shoulder heavy burdens to address the government's specific fears. In particular, online intermediaries might face the choice of either cooperating with the local authorities to address relevant fears, or exiting the market. Though the liability of offshore online intermediaries that provide services to Vietnamese users on a cross-border basis currently remains ambiguous in certain cases, the same trend may soon apply to those intermediaries as well. However, in contrast to this trend toward heavy regulation, the specific commitments of Vietnam under applicable international trade arrangements may, to a certain extent, restrain Vietnamese discriminatory regulatory measures towards foreign online intermediaries.

For the readers' ease of reference – before going into detailed analysis – this essay provides a brief overview of key regulations concerning online intermediaries in Vietnam in Figure 1 and basic facts about the Internet in Vietnam in Figure 2 below.

Key regulations concerning online intermediaries in Vietnam

Under the Vietnamese legal system, laws are adopted by the General Assembly of Vietnam. Decrees are issued by the Government to implement adopted laws. An adopted decree can then be further detailed by circulars of a specific responsible ministry or by joint-circulars of multiple ministries. Only when a regulation has been adopted, it is assigned with a number. This essay refers to a regulation that has not been adopted as a "draft" regulation. Key regulations mentioned in this essay include the following:

1. **Law on Information Technology** (IT Law) – (adopted in 2006, currently still in effect)
   - Promotes the application and development of information technology in various fields, including in

governmental operation and in commerce.

- Makes online intermediaries liable for actively contributing to the production and distribution of the illegal content, such as generating, curating, or modifying the content; and explicitly exempts online intermediaries from liabilities in certain circumstances. (Arts. 16.4, 17.2)
- Provides that entities applying information technologies are not responsible for tracking or monitoring digital information of third parties, or investigating infringing acts of third parities while transmitting or storing their information. (Art.20.2)
- Requires online intermediaries to undertake necessary measures to block the access to or remove illegal information at authorities' requests. (Arts. 16.3, 18.3, 19.3, and 20)
- Contains principles on protecting personal information (Arts. 21 and 22); similar principles are stated under the Civil Code (adopted in 2005, Arts. 31 and 38); Law on e-Transaction (adopted in 2005, Art. 46), and the Law on Protection of Consumers' Rights (adopted in 2010, Art.6).

2. **Press Law** (adopted in 1989, amended in 2002, currently still in effect)

- Defines press as "the mouthpiece of Party organizations, state bodies and social organizations, and a forum for the people." (Art. 1)
- A license is required to operate as a press agency in Vietnam; only limited entities are eligible to apply for a license. (Art. 6, Decree No. 51 implementing the Press Law)
- Certain activities, which are vaguely defined, are prohibited. Included in the definition of prohibited behaviors and acts are, "seditious, libelous, defamatory, obscene and violent, and those that constitute hate speech or disclose State secrets." (Art. 10) The Law on Publication (both 2012 and 2004 versions) contains a similar list of prohibited activities.

3. **Decree No. 72** on Management, Provision, and Use of Internet Services and Online Information (adopted in 2013 to replace Decree No. 97, which was adopted in 2008 and replaced Decree No. 55 below)

- Requires owners of social networking sites and general news sites to get a license from a government agency before starting operation, locate at least one server in Vietnam, and make available information safety and security protection measures. (Arts. 23.4, 23.5(a) & (d), 24.1 and 25.8.)
- Online intermediaries "are held liable for actively contributing to the production and distribution of the illegal content, such as generating, curating, or modifying the content." (Art. 25.5.)
- Requires online intermediaries to coordinate with authorities in blocking prohibited content. (Art. 25.6)
- Restricts the activities of bloggers and users of online social networking sites to the provision and exchange of information of their own, not third parties'. (Art. 20.2)
- Requires that online social network service suppliers ensure that only individuals who have supplied "accurate and complete personal information as required by law", including the government-issued identity card number, may create blogs or provide information on online social networks. (Arts. 3.16 and 25.9)
- When Decree No. 72 was still a draft regulation, there was a tentative proposition that offshore providers of public information - if they serviced a large amount of users in the territory of Vietnam - must establish representative offices or appoint legal representatives in Vietnam. When adopted, Decree No. 72 vaguely provides that foreign suppliers of "public information across the border, which are used in Vietnam or accessed from Vietnam, shall comply with Vietnam's relevant laws. The Decree also defers to the MIC for detailed guidance on the provision of public information across the border. (Art. 22).
- The Decree also expressly recognizes the economic benefits of Internet activities and confirms the policy of promoting the use of Internet to raise productivity, create jobs, and improve quality of life. (Arts. 4.1 and 4.2)

4. **Decree No. 55** on Management, provision and use of Internet services (adopted in 2001, **replaced by Decree No. 97** in 2008, which itself was replaced by Decree No. 72 above in 2013)

- Explicitly acknowledged the role of Internet services to Vietnam economic development (Arts. 3 and 5).
- This Decree introduced OSP's or Online Service Providers, as a category of service provider in 2001. OSPs provide application services, and are only subject to regulation through "specific State management agencies" (Art. 36). This makes OSPs different from IXPs, ISPs, and ICPs, which are subject to the licensing requirements directly provided by Decree No. 55.
- Expressly permitted the use of Internet application services of both domestic and foreign OSPs (Art. 22.2).

- Decree No. 55 also contained provisions requiring online intermediaries to block prohibited content (Art. 7.1).

5. **Decree No. 21/CP** regarding the Promulgation of "Temporary Regulation on the Management, Establishment, and Use of the Internet in Vietnam" (issued in 1997, **replaced by Decree No. 55**)

- Subjected online content to the regulations on press and publication; contained general descriptions of types of content that cannot be transmitted on the Internet; and required online intermediaries to block prohibited content. (Art. 3)
- Contained strict regulations on the use of the Internet by the Party, the government, public security and national defense function agencies: establishment of secured private network, encryption of information, prevention of data thief and unauthorized access. (Art. 20)
- All organizations wishing to connect to the Internet, either for private use or for commercial purpose, must locate their servers in Vietnam and to connect to the Internet through a limited number of government-licensed international gateways. (Arts. 1 and 12)
- IXPs, ISPs, and ICP must obtain written permission from designated governmental agencies before connecting to the Internet. (Art. 5)
- Individual users had to enter into contracts for Internet services from local ISPs and must be responsible for the content they receive and deliver. (Art. 12)
- It was illegal to use telephones, private leased lines, and other connection methods for accessing the Internet though an offshore server. (Part IV, Section 4, Item 3 of Joint Circular 08, which guided the implementation of certain provisions of Decree No. 21)
- The government also controlled the identification of Internet users by demanding periodical and irregular reports of the same information from ISPs. (Part IV, Section 2, Item 6 of Joint Circular 08, which guided the implementation of certain provisions of Decree No. 21)

6. Decree No. 52 on E-commerce (issued in 2012, currently still in effect)

- E-commerce business website owners, including foreign or cross border owners, must disclose their identities.
- Owners of e-commerce business websites and e-commerce service websites, including foreign owners using *.vn* domain name, must respectively conduct notification and registration procedures with the Ministry of Industry and Trade. (Arts. 2.1(c), 27.1, 36.1, 41.1, 46.1, and 55.1)
- Emphasizes transparency in e-commerce by requiring the disclosure of certain information for specific types of websites. (Arts. 28-34)
- Includes a broad range of prohibited acts .(Art. 4)
- Recognizes the validity of electronic evidence, confirms the effectiveness of online contracts, and introduces mechanisms to rate websites' creditability and data protection policy, and to authenticate electronic contracts. (Arts. 9-14, 15-23, 60-63)
- Owners of websites with online payment functions and suppliers of online payment services are subject to specific obligations under Decree No. 52 regarding the safety and confidentiality of online payment transactions. They may be held jointly liable for any damage caused by the illegal disclosure, amendment, reproduction, cancellation, deletion, or transfer of online payment information via the website. In addition, website owners who develop their own online payment solutions to support the online sale of their goods must apply specific measures to ensure safety and confidentiality of customer data. (Arts. 74 and 75)

7. Joint Circular No. 07 on the Liabilities of Intermediary Service Suppliers in Protection of Copyrights and Related Rights on the Internet and Telecommunications Network Environment (issued in 2012, currently still in effect)

- Online intermediaries are directly liable for infringing content only in limited circumstances, e.g. when they initiate the posting, transmission or provision of the infringing content over the Internet or telecommunications network, modify or copy the infringing content, deliberately circumvent technology measures applied by right owners to protect copyrights or related rights, or operate as the secondary distributors of the infringing content. (Arts. 3.1 and 5)

8. Draft Decree on Information Technology (IT) Services (not yet issued)

- As of April 25, 2014, the MIC has made three different versions of the Draft Decree available to the public: the first was made available in 2010, the second in April 2012 ("April 2012 version") and the third on August 3, 2012 ("Version 3.8"). This essay focuses on the last two versions.

- The April 2012 version required that the servers and infrastructures for the provision of certain IT services must be located in Vietnam, including cloud computing services, web search portal services, and database center services. (Art. 15) This localization requirement was removed from Version 3.8.
- The April 2012 version prohibited cross-border supply of certain services, including web search portal services, cloud computing services, and database center services and required foreign service suppliers to establish a local entity and locate their servers in the territory of Vietnam in order to be eligible for an operation license in Vietnam (Arts. 15 and 20.1). The Version 8.3 modified the April 2012 version such that cross border supply of cloud computing services, database center services, and web search portal services is permitted provided that they do so through local branches or local intermediaries. (Art. 19.3)

9. <u>Draft circular detailing certain provisions of Decree No. 72</u> (not yet adopted)

- Requires that for authentication purpose, the online social network service supplier must link the ID number provided by the user to the national online database on personal information at the authority's request. (Art. 3.2)

***Figure 1**. Key regulations concerning online intermediaries in Vietnam*

Basic facts about Internet in Vietnam

- The Internet came to Vietnam in the early 1990s.
- By June 30, 2012, Vietnam had 31 million Internet users (equivalent to over 33% of Vietnamese population), ranking within the top 10 countries in the Asia-Pacific Region in terms of Internet growth. (Vietnam ICT White book 2013)
- Facebook, Google's search engine, YouTube, Gmail, and Yahoo! Mail are among the most popular online tools for Vietnamese users.
- Access to Facebook in Vietnam has been on and off since 2009. The alleged blocking can be bypassed by using a proxy server or a virtual private network, or by changing their DNS.
- In 2013, at least 46 bloggers or democracy activists were convicted and imprisoned on national security charges. (Associated Press (Oct 29, 2013)).
- In May 2014, Microsoft Security Intelligence Report announced Vietnam as one of the top five countries with the highest rates of malware affection. (PC World VN (May 17, 2014))
- Estimated turn over of the digital advertising market in Vietnam was $32 million and it is expected to reach $45 million by 2015. (VietnamNet, Dec. 3, 2013)
- Expected total revenues of Internet services and content to be VND 100 trillion (approximately USD 47 billion) by 2018. (VietnamNet, Dec. 3, 2013)
- Key strategies of the Vietnamese governments:
  + Boosting e-commerce to enhance national enterprises' competitiveness. (General Plan for the Development of Electronic Commerce in the 2011-2015 Period, approved by the Prime Minister of Vietnam on Jul. 12, 2010)
  + Promoting IT training, applications, and developments; providing basic governmental services online, applying information technology in management, operation, and business operation of 80% enterprises and social organizations, universalize IT application in the education and healthcare system, and enhance the application of IT in national defense and security. (The "Soon Turning Vietnam into a Strong Nation in Information Technology and Communications" Project, approved by the Prime Minister of Vietnam on Sept 22, 2010)
  + Promoting the development of Vietnam ICT brand-name products and services (VIBrand). (Vietnam ICT White book 2012)

***Figure 2.** Basic facts about Internet in Vietnam*

II. Analysis

A. Regulations Responding to Fears

This section analyzes different sets of fears to illustrate their effect on the liabilities of online intermediaries in Vietnam. The country shares with other nations common fears regarding the Internet, including its possible effects on national security, online fraud prevention, data and privacy protection, and network security. However, the regime also demands specific regulations to address fears relating to uncontrollable content. Furthermore, Vietnam also worries about failing to capture domestically the financial benefits generated by foreign online intermediaries through their online activities in Vietnam. All of these fears result in a stringent liability regime for online intermediaries, the chokepoints of Internet activities.

1. Untested Internet in 1990s– Maximize Government Control Over Online Activities

Originally, the government's concerns were related to the unprecedented nature of the Internet as a new technology, the benefits of which were untested in Vietnam. As a result, in the 1990s, regulations were of a cautious and exploratory nature, and Internet activities were permissible only to the extent that they were navigable and controllable by the government.

In particular, the domestic Internet architecture was designed in such a way that the local authority had full control over domestic online activities: all organizations wishing to connect to the Internet, either for private use or for commercial purposes, were required to locate their servers in Vietnam and to connect to the Internet through a limited number of government-licensed international gateways.[6]

Internet exchange providers (IXPs), Internet service providers (ISPs), private organizational Internet users, and Internet content providers (ICPs) had to obtain written permission from designated governmental agencies before connecting to the Internet.[7] Individual users had to enter into contracts for Internet services from local ISPs.[8] It was illegal to use telephones, private leased lines, and other connection methods for accessing the Internet though an offshore server.[9] The government also controlled the identification of Internet users by demanding periodical and irregular reports of the same information from ISPs.[10]

From the above structure, the government of Vietnam targeted IXPs, ISPs, private organizational Internet users, and ICPs as the chokepoints to control domestic Internet activities. This early

6 See Nghị định của Chính phủ số 21/cp ngày 5 tháng 3 năm 1997 về việc ban hành "Quy chế tạm thời về quản lý, thiết lập, sử dụng mạng Internet ở Việt Nam" [Decree No. 21/CP regarding the Promulgation of "Temporary Regulation on the Management, Establishment, and Use of the Internet in Vietnam," issued by the Government of Vietnam on March 5, 1997], replaced by decree No. 55/2001/nd-cp in 2001, (Viet.) (hereinafter "Decree No. 21"), Art. 1.

7 See Decree No. 21, Art. 5.

8 See id., Art. 12.

9 See Thông tư liên tịch Tổng Cục Bưu điện – Bộ Nội vụ - Bộ Văn hoá Thông tin số 08/TTLT ngày 24 tháng 5 năm 1997 Hướng dẫn Cấp phép việc Kết nối, Cung cấp và Sử dụng Internet ở Việt Nam [Joint Circular between the General Postal Department, Ministry of Internal Affairs, and Ministry of Culture and Information No. 08/TTLT dated May 24, 1997, Guiding the Licensing Procedures for the Connection, Provision and Use of the Internet in Vietnam], Part IV, Section 4, Item 3 (Viet.).

10 See id., Part IV, Section 2, Item 6.

model of heavy Internet control enabled the maximum local regulatory sovereignty, which, as discussed below, also closely resembles the current nature of Vietnamese Internet regulations.

2. Fear of Uncontrollable Content - Heavy Censorship

The second set of fears relates to the ideology of the current Vietnamese regime. The Internet and the availability of online platforms enabled by various online intermediaries changed the nature of traditional journalism and content production in general: every user can easily generate content, the number of Internet users has increased immensely globally, creating a massive audience for online content, and the platforms hosting this content can be provided on a cross-border basis. Furthermore, as demonstrated by the Arab Spring, online platforms may serve as an effective means to mobilize social forces against the government. This is exactly the kind of risk in relation to online intermediaries that the current Vietnamese regime would like to prevent.[11] In such a context, controlling content – particularly that which conflicts with the communism ideology – at the user level is no longer the most efficient approach. Thus, the local authority has turned its censorship focus to online intermediaries – the Internet chokepoints. This new focus has resulted in intensive obligations being imposed on online intermediaries. However, it appears that due to international trade law obligation constraints, among other things, some of the proposed requirements have not been adopted.

i. Exclusive "Mouthpiece" – Challenges on Censorship in the Internet Era and the Call for Censorship Innovations

Unlike the press in the United States, which is treated as the "fourth estate," providing "a public check on the three classes of branches of government,"[12] the press in Vietnam is defined as the "mouthpiece of Party organizations, State bodies and social organizations, and a forum for the people."[13] Accordingly, only Party organizations, State bodies, and social organizations are eligible for a license to establish a press agency in Vietnam.[14] Certain vaguely defined types of content are strictly prohibited, including those that are seditious, libelous, defamatory, obscene and violent, and those that constitute hate speech or disclose State secrets.[15] A similar set of content was also prohibited from publication and distribution, including electronic publication and distribution, according to the Law on Publication.[16]

---

11 Charlie Campbell, Internet Censorship is Taking Root in Southeast Asia, Time (Jul. 18, 2013), http://world.time.com/2013/07/18/Internet-censorship-is-taking-root-in-southeast-asia/#ixzz2uP36ZHbs.

12 "US vs Bradley Manning, Volume 17 July 10, 2013 Morning Session", Freedom of the Press Foundation: Transcripts from Bradley Manning's Trial, 29, July 10, 2013, https://pressfreedomfoundation.org/sites/default/files/07-10-13-AM-session.pdf.

13 Luật Báo Chí [Press Law] adopted by the National Assembly of Vietnam on December 28, 1989, (Viet.) (hereinafter "Press Law") Art. 1.

14 Nghị định của Chính phủ số 51/2002/NĐ-CP ngày 26 tháng 4 năm 2002 Quy định chi tiết Thi hành Luật Báo chí, Luật sửa đổi, bổ sung một số điều của Luật Báo chí [Decree of the Government No. 51/2002/ND-CP dated April 26, 2002 Providing Detailed Guidance on the Implementation of the Press Law, the Law Amending Certain Provisions of the Press Law] (Viet.) (hereinafter Decree No. 51), Art. 6.

15 See Press Law, Art. 10; See also Decree No. 51, Art. 5.

16 Luật Xuất bản [Law on Publication] No. 19/2012/QH13, adopted by the National Assembly on November 20, 2012 (Viet.) (hereinafter "Publication Law"), Art. 10.1. The same languages were also included in previous version of the Publication Law such as Law No. 30/2004/QH11 dated December 3, 2004, Art. 10.

The Internet, as observed by Yochai Benkler, changed the nature of traditional journalism.[17] Thanks to the reduction of production and distribution costs, every individual Internet users with basic computer skills can nowadays generate and proliferate content on the Internet in a matter of seconds. In fact, online social networking websites, such as Yahoo! 360 in the past and Facebook currently, are popular platforms for Vietnamese individuals to exchange online information and directly generate online content. They discuss political and economic topics, criticize governmental policies, spread the news, and gather to demonstrate against such policies, among other things.[18] Some of these activities were treated as libelous and seditious, and in violation of Vietnamese laws.

For example, in 2013, at least 46 bloggers or democracy activists were convicted and imprisoned on national security charges.[19] In particular, a Facebook user was sentenced to 15 months of house arrest for posting and exchanging false and distorting information, and harming the Government's reputation, as well as the legitimate rights of organizations and citizens in October 2013.[20]

Since the introduction of the Internet in Vietnam, the government has insisted that all Internet users must be responsible for the content they deliver and receive online.[21] The law also consistently requires IXPs, ISPs, online service providers (OSPs), ICPs, and Internet service agents to act as gatekeepers in adopting appropriate measures to block the prohibited content defined under the Press Law and the Publication Law, among others.[22] However, a number of challenges have emerged over time, demanding regulatory innovations by the Vietnamese Government.

---

17 Yochai Benkler, A free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate, Harvard Civil Rights-Civil Liberties Law Review, Winter 2012, Vol. 47 Issue 1, 311, at 371-379.
18 See H.C., Facebook in Vietnam - Defriended, The Economist (Jan. 4, 2011, 17:46), http://www.economist.com/blogs/banyan/2011/01/facebook_vietnam.
19 Vietnam Court Convicts Dissident Facebook User, Associated Press (Oct 29, 2013, 02:27:32), http://bigstory.ap.org/article/vietnam-court-convicts-dissident-facebook-user.
20 The charge against this Facebook user was "abusing democracy and freedom rights, causing harms to the Government's interest and the legitimate rights and interest of organizations [and] citizens." His activities were the effort to overturn his brother's conviction for anti-government propaganda. See Vietnamplus, Tuyên phạt 15 tháng tù treo đối tượng Dinh Nhật Uy [Sentencing 15 Months of House Arrest Against Dinh Nhat Uy], VTV, (Oct. 29, 2013, 22:12), http://vtv.vn/Thoi-su-trong-nuoc/Tuyen-phat-15-thang-tu-treo-doi-tuong-Dinh-Nhat-Uy/87378.vtv. See also Martin Petty and Robert Birsel, Vietnam Court Sentences Facebook Campaigner to House Arrest, Reuteurs (Oct. 29, 2013, 5:21 AM), http://www.reuters.com/article/2013/10/29/us-vietnam-court-idUSBRE99S0DP20131029.
21 See Decree No. 21, Arts. 1 and 12.
22 See Decree No. 21 Art. 3; Nghị định 55/2001/NĐ-CP ngày 23 tháng 8 năm 2001 về Quản lý, Cung cấp và Sử dụng Dịch vụ Internet [Decree No. 55/2001/ND-CP dated August 23, 2001 regarding the Management, Provision and Use of Internet Services], replaced by decree No. 97/2008/ND-CP IN 2008 (Viet.) (hereinafter "Decree No. 55"), Arts. 3.1 and 7.1; IT Law, Arts. 16.3, 18.3, 19.3, and 20; Nghị định của Chính phủ số 97/2008/NĐ-CP ngày 28 tháng 8 năm 2008 về Quản lý, Cung cấp, Sử dụng Dịch vụ Internet và Thông tin Điện tử trên Internet [Decree No. 97/2008/ND-CP of the Government dated August 28, 2008 on Management, Provision, and Use of Internet Services and Electronic Information on the Internet], replaced by decree No. 72/2013/nd-cp in 2013 (Viet.) (hereinafter "Decree No. 97"), Art. 10.2(c), 11.2(c), 21.1(c); Nghị định Quản lý, Cung cấp, Sử dụng Dịch vụ Internet và Thông tin trên mạng [Decree on Management, Provision, and Use of Internet Services and Online Information] No. 72/2013/ND-CP dated July 15, 2013 (Viet.) (hereinafter "Decree No. 72"), Art. 25.6;

The first challenge involved the immense increase in the number of Internet users in Vietnam. By June 30th, 2012, Vietnam already had 31 million Internet users, ranking within the top 10 countries in the Asia-Pacific Region in terms of Internet growth.[23] Although the Internet allows for the tracing of IP addresses, this tracing is not perfect. It is difficult to be certain of the real identity of an Internet user.[24] For example, Facebook users must be 13 years or older, and alcohol advertisement is prohibited for minors under 18 years old. Unlike the face-to-face communications outside the Internet world, there is currently no perfect mechanism to authenticate online whether the person acquiring the service for the first time is declaring his or her real age. Thus, illegal content may be available on the Internet beyond the government's ability to regulate.

Secondly, many major online platforms are made available in Vietnam by foreign, rather than domestic, service suppliers. Since 2001, Vietnam has explicitly permitted the use of Internet application services of both domestic and foreign OSPs.[25] As a result, foreign-based services such as Facebook, Google's search engine, and YouTube are among the most popular online tools for Vietnamese users. These services are supplied on a cross-border basis without establishing any local presence in Vietnam. This feature raises additional challenges to the Vietnamese regulator's content control efforts. As a result, the government has demanded mechanisms to control online activities that take place not only via locally licensed online intermediaries, but also via popular offshore online intermediaries.

The Facebook blocking that began in 2009 represented one of the first responses against offshore online intermediaries who provide services on a cross-border basis in Vietnam. Although the government denied its involvement in the blocking, an unsigned official letter was circulated on the Internet bearing the instruction of a Department under the Vietnamese Ministry of Public Security for ISPs.[26] Accordingly, ISPs were required to block a list of eight websites, including Facebook. Immediately following the date of that letter, Vietnamese users faced difficulties[27] accessing Facebook. With or without the government's involvement, and regardless of the potential motivations behind this move (discussed further in the next section), this blocking was just the beginning of a much more systemic attempt to censor Internet content, signaling stricter burdens would be imposed on online intermediaries – the chokepoints in controlling online content. A series of regulations and draft regulations proposed since 2012 illustrate this attempt by the government of Vietnam, discussed below.

ii. More Censorship on Internet Chokepoints

23 See National Steering Committee on ICT (NSCICT) and Ministry of Information and Communications (MIC), White Book 2013: Vietnam information and communication technology, Information and Communications Publishing House, (2013), at 22.

24 For a comparison between identity authentication in the Internet and that in real space and for more discussion on the relationship between users' identification and the "regulability" of the Internet, see Lessig, at 38-60.

25 Decree No. 55, Art. 22.2.

26 The letter is available on Wikileaks at this link: http://file.wikileaks.org/file/vietnam-banned-facebook.jpg (last visited April 10, 2014) (Viet.).

27 Though there were some inconveniences in accessing Facebook following the alleged blocking, the blocking was easily circumvented by using certain proxy techniques. The access speed varied among ISPs and accession via mobile phones was not affected. Please see further discussion and explanation in the next section of the essay.

In general, online intermediaries must remove or block access to the prohibited content that they self-detect or per the request of the competent authority in Vietnam.[28] They are held liable for actively contributing to the production and distribution of the illegal content, such as generating, curating, or modifying the content.[29]

Decree No. 72, adopted in July 2013,[30] in line with the traditional Vietnamese command and control regulatory model, requires owners of online social networking websites and general news websites[31] to obtain a license from the government agency before providing their services.[32] Notably, the licensee must satisfy certain conditions including, among other things, being established under Vietnam law,[33] and having at least one server located in the territory of Vietnam.[34] Similarly, under these regulations, publishers and distributors of electronic publications must also locate their servers in Vietnam.[35]

Furthermore, the April 2012 version of the Draft Decree on Information Technology Services[36] required that the servers and infrastructure for the provision of certain IT services be located in Vietnam. These services include cloud computing services, web search portal services, and database center services.[37] This approach to a certain extent reflects the regulatory approach that Vietnam originally applied in the 1990s – maximizing domestic control over online activities. In other words, the server localization, among others, allows Vietnam to effectively exercise its sovereignty over Internet activities in Vietnam.

The Vietnamese Government also adopted measures to limit user content sharing activities such that its regulatory scope can focus on the chokepoints − online intermediaries. In particular, Decree No. 72 restricts the activities of bloggers and users of online social networking sites to the provision and exchange of information of their own, not third parties' information.

---

28 See IT Law, Arts. 16.3, 18.3(b), 19.3 (regarding the liabilities of entities transmitting and disseminating digital information, leasing online storage, and providing digital information search tools); See also Decree No. 72, Arts. 24.4 and 25.6 (regarding obligations of general news websites and online social networking websites).

29 See IT Law, Art. 16.4 (providing cases where entities transmitting and disseminating electronic information are liable for illegal information); Art. 17.2 (providing cases where entities are liable for the information they temporarily store); See also Decree No. 72, Art. 25.5.

30 Nghị định Quản lý, Cung cấp, Sử dụng Dịch vụ Internet và Thông tin trên mạng [Decree on Management, Provision, and Use of Internet Services and Online Information] No. 72/2013/ND-CP dated July 15, 2013 (Viet.) (hereinafter "Decree No. 72").

31 "General news website" means websites that provides aggregated information about politics, economics, culture and/or society, on the basis of citing textually and accurately from official sources and specify the names of the authors or agencies of the official sources, and the time when such information is published. Decree No. 72, Arts. 3.19 and 20.2.

32 Decree No. 72, Art. 23.4.

33 See id. Art. 23.5(a).

34 See id. Arts. 24.1 and 25.8.

35 Nghị định Quy định Chi tiết Một số Điều và Biện pháp Thi hành Luật Xuất Bản [Decree Detailing Certain Provisions and the Implementation of the Law on Publication] No. 195/2013/ND-CP dated November 21, 2013, Art. 17.1(a).

36See Dự thảo Nghị định về Dịch vụ Công nghệ Thông tin [Draft Decree on Information Technology Services], Apr. 2012, available at http://qtsc.com.vn/c/document_library/get_file?uuid=63cd7c9e-065c-4f06-a6a0-93ab819b7ce2&groupId=18, (last visited Jan. 1, 2014) (Viet.), (hereinafter "April Version").

37 See April Version, Art. 15. The same requirements was removed from the latest publicly available version of this Draft Decree. See the collection of version 3.8 of the Draft Decree and a set of comments in both English and Vietnamese, http://www.vibonline.com.vn/Duthao/1250/Nghi-dinh-ve-dich-vu-cong-nghe-thong-tin.aspx, (last visited Jan. 1, 2014).

Accordingly, permissible activities do not include "posting aggregated information."[38] This provision seems to address the issue of content "curation," as commonly referred to in other jurisdictions**.** In response to the accusation that this provision restricts freedom of speech, a representative of the Ministry of Information and Communications ("MIC") called the accusation a "misunderstanding" and clarified that Vietnam "never bans people from sharing information or linking news from websites."[39] Rather, the provision "was aimed at protecting intellectual property and copyright" [relating to the posting of aggregated information].[40] In an interview with VOV, MIC Deputy Minister called the accusation a "quibble," and argued that the provision was actually helpful in guiding users as to the boundary of their online activities for their ease of compliance.[41]

Regardless of whether the above provision restricts freedom of speech, it has an important direct effect with respect to which sites or individuals are subject to regulation. Particularly, once a blogger or a user of online social networking sites posts aggregated information, their websites will likely be treated as a general news website, which are subject to the licensing requirement mentioned above. This licensing procedure serves both as a mechanism for the government to review and evaluate the capability of every applicant, and as a burden that discourages individual users from posting aggregated information. Since only licensed owners of general news websites can post aggregated information, the government does not have to extend their control over aggregated information content beyond this limited group of licensees (such as bloggers posting aggregated news on their blogs).

Furthermore, besides the traditional requirement for coordination from gatekeepers, the Government of Vietnam is currently attempting to take one step further to directly control users' activities on online social networks. Specifically, Decree No. 72 requires that online social network service suppliers ensure that only individuals who have supplied "accurate and complete personal information as required by law," including the government-issued identity card number, may create blogs or provide information on social networks.[42]

The draft circular implementing Decree No. 72 further requires that for authentication purposes, the supplier must link the ID number provided by the user to the national online database on

38 Decree No. 72, Art. 20.2. "Aggregated information means information that is collected from multiple sources and types of information about politics, economics, culture and/or society." Decree No. 72, Art. 3.19.
39 Vietnam Rebuffs Criticism of 'Misunderstood' Web Decree, Reuters (Aug. 6, 2013, 7:53), http://www.reuters.com/article/2013/08/06/vietnam-Internet-idUSL4N0G72IA20130806
40 Id.
41 Hương Giang, Nghị định 72 Không Hạn chế Quyền Tự do Ngôn luận [Decree No. 72 Does Not Restrict Freedom of Speech], VOV (Aug. 7, 2013, 16:41), http://vov.vn/Xa-hoi/Nghi-dinh-72-khong-han-che-quyen-tu-do-ngon-luan/274653.vov (VOV reporter interviewed the Deputy Minister of Information and Communications, Mr. Do Quy Doan, regarding the provision of Decree No. 72).
42 Decree No. 72, Arts. 3.16 and 25.9.

personal information at the authority's request.[43] The national online identification database is still a work in-progress, thus this requirement is not enforceable until the database is fully developed.[44] However, once implemented, this ID verification scheme will possibly make the Internet users' behaviors more - in Lawrence Lessig's words - "regulable".[45] Verification will in theory prevent crimes, frauds, and defamation as well as promote trust on the online environment, which is good for e-commerce.[46]

Nevertheless, at the same time, the required disclosure of users' real identity may effectively contribute to the suppression of freedom of speech.[47] For example, the awareness that speech can directly link to a real identity will hinder users from expressing anti-government and other controversial opinions, and may even discourage them from expressing opinions at all due to the risk of liability. This choice of architecture reflects a value choice by the government. Obviously, freedom of speech is not the government's priority in this case. Rather, online intermediaries' compliance with this requirement will likely enable the government to regulate the Internet more effectively at the cost of freedom of speech.

So far, the liabilities of offshore online intermediaries that provide services to Vietnamese users on a cross-border[48] basis are still ambiguous. When Decree No. 72 was still a draft regulation, there was a tentative proposition that offshore providers of public information – if they serviced a large amount of users in the territory of Vietnam – must establish representative offices or appoint legal representatives in Vietnam.[49] Similarly, the April 2012 version of the Draft Decree on IT Services prohibits cross-border supply of certain services, including web search portal services, cloud computing services, and database center services.[50] Rather, in order to provide

---

43 See Dự thảo Thông tư Quy định Chi tiết Một số Điều của Nghị định 72/2013/NĐ-CP Ngày 15 tháng 7 năm 2013 về Quản lý, Cung cấp, Sử dụng Dịch vụ Internet và Thông tin Trên mạng Đối với Hoạt động quản lý trang thông tin điện tử và dịch vụ mạng xã hội [Draft Circular Detailing the implementation of Certain Provisions regardingManagement of General News Websites and Online Social Networking Services of Decree No. 72/2003/ND-CP dated July 15, 2013 on the Management, Provision and Use of Internet Services and Online Information], Art. 3.2(b), downloadable at http://mic.gov.vn/Attachment%20Lay%20Y%20Kien%20Nhan%20Dan/Du%20thao%20thong%20tu%20MXH%20(Du%20thao%203%20ngay%204.%209).doc (last visited April 25, 2014).

44 Lê Mỹ, Chưa Bắt Doanh nghiệp Xác thực Chứng minh thư Thành viên Mạng Xã hội [Not Yet Requiring Enterprises to Verify the Identification of Online Social Network Users], ICTNews (Jan. 10, 2014, 16:52), http://ictnews.vn/Internet/chua-bat-doanh-nghiep-xac-thuc-chung-minh-thu-thanh-vien-mang-xa-hoi-114111.ict.

45 Lawrence Lessig, Code is Law 2.0, at 16.

46 Lessig found this crucial for e-commerce. However, the identification authentication that Lessig foresees as the "most important tool for identification in the next ten years" is far different from the proposed requirement of the Vietnamese government. He endorses the technology that can verify specific users' information for specific online purposes; but the disclosure of users' identities to the authorities requires warrant. See Lessig at 50-54.

47 For a succinct summary of the importance of pseudonymity, see Mike Masnick, What's In A Name: The Importance Of Pseudonymity & The Dangers Of Requiring 'Real Names', TECHDIRT, (Aug. 5, 2011; 6:36 PM.) https://www.techdirt.com/articles/20110805/14103715409/whats-name-importance-pseudonymity-dangers-requiring-real-names.shtml.

48 The cross-border supply of a service occurs when the service supplier is not present within the territory of Vietnam but the service is delivered in Vietnam. See the Guidelines for the Scheduling of Specific Commitments under GATS, S/L/92 (28 March 2001)

49 See Dự thảo Nghị định Quản lý, Cung cấp, Sử dụng Dịch vụ Internet và Nội dung Thông tin Trên Mạng [Draft Decree on Management, Provision, [and] Use of Internet Services and Network Information Content], the third version, available at http://mic.gov.vn/layyknd/trang/dựthảonghịdinhInternet.aspx, (last visited April 20, 2014) (Viet.).

50 See April Version, Art. 20.1.

the relevant services in Vietnam, the foreign service suppliers must establish a local entity and locate their servers in the territory of Vietnam in order to be eligible for a license.[51] These proposed regulations, if adopted as such, would effectively extend Vietnamese local regulatory power to a broad range of otherwise cross-border Internet activities in Vietnam, similar to the state of affairs in the 1990s (as discussed above).

iii. Censorship and International Trade Law Constraints

However, in the current context of Vietnam, there are international factors that may restrain the successful implementation of the above regulatory structure.

In particular, since 2000 Vietnam has entered into a number of international trade arrangements, in which the commitments by Vietnam constitute restraints or prohibitions against market access limitations of this type. Key international trade arrangements include the Bilateral Trade Agreement between Vietnam and the U.S. in 2000, Vietnam's World Trade Organization membership beginning in 2007, and a number of regional trade agreements through the ASEAN.

As a part of these trade arrangements, Vietnam made market access commitments on specific service sectors, including telecommunications services, computer and related services, distribution services, and advertising services, among others.[52] Accordingly, Vietnam cannot impose any form of market access limitations[53] on the cross-border supply of a specific service included in its Service Schedule unless the limitation is explicitly mentioned in the Service Schedule or such restrictions justify the exemptions provided under the applicable trade agreement.[54] For example, where online services are included in Vietnam's Service Schedule and no market access limitation was explicitly reserved therein, a prohibition against cross-border supply of these services might violate Vietnam's obligations under the relevant international trade agreements.

The above context might explain why Decree No. 72 vaguely provides that foreign suppliers of "public information across the border, which are used in Vietnam or accessed from Vietnam, shall comply with Vietnam's relevant laws."[55] The Decree also deferred to the MIC for detailed provisions on the provision of public information across the border.[56] Similarly, the April 2012 version of the Draft Decree on IT Service removed the prohibition against the cross border supply of cloud computing services, database center services, and web search portal services. Rather, foreign suppliers are permitted to provide these services on a cross-border basis as long as that they do so through local branches or local intermediaries. Although the consistency of this revised provision with Vietnam's international trade commitments is still questionable, if adopted as such, it will likely serve as one of the new mechanisms for the government to exercise their control over the content provided through cross-border online intermediaries' services. In such cases, the local presences, local partners or agents of the foreign online intermediaries will

51 See April Version, Arts. 15 and 20.1.

52 See for example, the World Trade Organization, Working Party on The Accession of Viet Nam, Schedule CLX – Vietnam, Part II – Schedule of Specific commitments in Services, WT/ACC/VNM/48/Add.2 (Oct. 27, 2006), available at http://www.wto.org/english/thewto_e/acc_e/a1_vietnam_e.htm.

53 There are six specific forms of market access limitation listed under the GATS Art. XVI.2.

54 See GATS, Arts. XVI (providing the principle on market access) and Art. XIV (providing the general exceptions which allow WTO members to maintain or adopt measures that are inconsistent with GATS principles).

55 Decree No. 72, Art. 22.1.

56 Decree No. 72, Art. 22.2.

have to comply with the authority's requirement, and thus directly lend assistance to the authority in controlling Internet content.

In short, this section explains how ideology protection and content censorship needs shaped the regulation of online intermediaries in Vietnam. The vast increase in the volume of Internet users plus the popularity of online platforms, which are hosted both in Vietnam and overseas, have recently required the government to exercise their extensive control at the online intermediary level. A number of regulations have been put in place and some additional measures are being proposed to realize this objective. As such, online intermediaries are expected to comply with more and more local requirements, which hopefully will be within the scope of the international trade commitments of Vietnam.

3. Traditional Fears

Like many other countries in the world, the Vietnamese government has concerns regarding the risks the Internet poses to national security, online transaction frauds, data privacy, and network security. These fears also contribute to more stringent regulations against online intermediaries.

i. National Security Risks

Since the 1990s, the government has set strict regulations on the use of the Internet by the Party, the government, public security, and national defense function agencies. Specifically, a private network must be established for Internet connection, the information flow on the network must be encrypted, and efficient technical measures must be applied to prevent data thief or unauthorized access that may cause harm to the system. Furthermore, the communications on the network must be controllable.[57] The recent revelation of NSA surveillance programs such as PRISM[58] and MUSCULAR[59] raised even more concerns regarding the exposure to national security risks through Internet use. The requirement of server localization imposed on certain forms of online intermediaries, among other things as discussed above, also serves as an effort to respond to this set of concerns.

ii. Online Fraud

Together with the growth of e-commerce activities in Vietnam, alarming scams and frauds have also emerged that demand regulation. The Vietnamese market has grown to include various

[57] Decree No. 21, Art. 20.

[58] PRISM enables NSA to collect data from U.S. electronic communications service providers according to the procedures provided under Section 702 of the Foreign Intelligence Surveillance Act (FISA) (50 U.S.C. §1881a). See Director of National Intelligence, Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, available at http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/871-facts-on-the-collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act, (last visited Jan. 22, 2014). Disclosed participants to this program include Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL, Apple. Data collected through PRISM include information content of all types, such as e-mails, videos, voices, photos, and online social networking details, etc. See The Washington Post, NSA Slides Explain the PRISM Data-Collection Program, published on June 6, 2013, updated on July 10, 2013, available at www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/, accessed on January 22, 2014.

[59] MUSCLAR program is a form of upstream data collection, which collects "communicatsions on fiber cables and infrastructure as data flows past." See Craig Timberg, The NSA Slide You Haven't Seen, The Washington Post, July 10, 2013, available at http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html?hpid=z1, accessed on 23 January 2014.

forms of online business, including online marketing and promotion, online sales, online auctioning, online payments, and online training, among others.[60] However, the issue of trust seems to drag down e-commerce development in the country. The concerns range from fraudulent online activities, deceptive advertisements, security for online payments, and e-signature and e-transaction validity.

For example, the *Muaban24* case involves a group of website owners who claimed to organize a trading platform for e-commerce services. Participants to this platform must contribute an initial amount of cash to own a virtual store on the website. The owners of the virtual store, instead of conducting any actual online trading activities on the stores, enjoyed a share of the money taken from every additional participant that they recruited.[61] The website owners themselves made money by also received a share of these payments.[62] Outside the online world, a similar business model for the sale of goods, as opposed to services, would constitute an illegitimate multi level marketing activity, (similar to a "pyramid scheme" in other jurisdictions), which is prohibited under the Competition Law of Vietnam.[63] Meanwhile, the company masked itself as an e-commerce business even in the absence of appropriate licenses from the authorities.[64] By August 2012, *Muaban24* had thousands of participants, sold 120,000 virtual stores, collected approximately USD30 million, and operated in 32 over 64 provinces in Vietnam.[65] The website owners were arrested and charged with "fraudulent appropriation of property" in numerous provinces.[66] This case has raised serious concerns regarding the effectiveness of State management as to online business activities, as well as trust issues surrounding e-commerce.[67]

---

[60] See Bộ Công Thương [Ministry of Industry and Trade], Báo cáo Thương mại Điện tử 2012 [2012 Report on E-Commerce] (December 2012), http://www.vecita.gov.vn/App_File/laws/3afc0508-107b-4ff4-9687-59b8a975cf79.PDF.

[61] See Vũ Văn Tiến - Hồng Kỹ, Vụ Muaban24: Cách thức Kinh doanh Đang Tạo Dư luận Tiêu cực [Muaban24 Case: A Business Model That Is Causing Negative Public Opinion], Dân Trí (July 28, 2012; 6:38), http://dantri.com.vn/ban-doc/vu-muaban24-cach-thuc-kinh-doanh-dang-tao-du-luan-tieu-cuc-623702.htm.

[62] See Vũ Văn Tiến - Hồng Kỹ, Các "Sếp Sòng" Muaban24 Kiếm Bao nhiêu Tiền? [How Much does Muaban24 "Chiefs" Have Earned?], Dân Trí (Aug. 4, 2012; 7:38), http://dantri.com.vn/kinh-doanh/cac-sep-song-muaban24-kiem-bao-nhieu-tien-626172.htm.

http://dantri.com.vn/event/muaban24-vu-an-rung-dong-2023.htm

[63] See Luật Cạnh tranh [Competition Law] No. 27/2004/QH11, adopted by the National Assembly of Vietnam on Dec. 3, 2004, Art. 48. Illegitimate multilevel marketing activities under this Law cover the marketing of goods only, not services.

[64] See Vũ Văn Tiến - Hồng Kỹ, Vụ Muaban24: Cách thức Kinh doanh Đang Tạo Dư luận Tiêu cực [Muaban24 Case: A Business Model That Is Causing Negative Public Opinion], Dân Trí (July 28, 2012; 6:38), http://dantri.com.vn/ban-doc/vu-muaban24-cach-thuc-kinh-doanh-dang-tao-du-luan-tieu-cuc-623702.htm.

[65] See id.

[66] See Hồng Kỹ - Vũ Văn Tiến, Bắt Khẩn cấp 4 Nhân vật Chóp bu Đường dây Muaban24 [Urgently Arrest 4 Top Personnel of Muaban24 Chain] (Aug. 2, 2012), http://dantri.com.vn/xa-hoi/bat-khan-cap-4-nhan-vat-chop-bu-duong-day-muaban24-625684.htm (regarding the arrest in Hanoi). See also An ninh Thủ đô, Tiếp tục Bắt giữ Nhiều Lãnh đạo Chủ chốt Của Muaban24 [Continue to Arrest Multiple Key Personnels of Muaban24] (citing Dân Trí) (Aug. 18, 2012), http://www.anninhthudo.vn/Phap-luat/Tiep-tuc-bat-giu-nhieu-lanh-dao-chu-chot-cua-Muaban24/460112.antd.

[67] See Group of Reporters, Thương mại Điện tử bị... Vạ lây vì Muaban24 [E-Commerce's Reputation Is …. Incidentally Hurt by Muaban24] (Aug. 5, 2012; 9:00), ICTNews, http://ictnews.vn/kinh-doanh/thuong-mai-dien-tu-bi-va-lay-vi-muaban24-104086.ict.

In addition, there were reported cases where intermediaries for online promotion and online group deals failed to remit service payment to service providers.[68] Users also complained about the quality of the services, which either failed to meet what was advertised or was subject to discrimination by the service suppliers.[69] Furthermore, a survey conducted by PayPal in 2012 revealed that 43% of those surveyed refrain from purchasing online due to risk concerns.[70]

Key factors contributing to the above issues include the immaturity of e-commerce activities in Vietnam, users' lack of awareness and experience, and ineffective enforcement of existing regulations. The government itself observed that many new forms of online business were "self-initiating" and blamed the above-mentioned situation to the "lack of strict surveillance by appropriate competent authorities."[71] Thus, it called for new specific regulations, noting in particular the fundamentally different nature of e-commerce transactions, where, unlike in-person transactions, buyers and sellers do not directly interact.

Decree No. 52[72] on e-commerce was part of the governmental efforts to address the above concerns. It is unclear to what extent the specific measures under Decree No. 52 may help improve trust and thus boost e-commerce activities in Vietnam. However, it is certain that under Decree no. 52 online intermediaries are subject to more compliance requirements. Specifically, owners of e-commerce business websites[73] and e-commerce service websites[74] must respectively conduct notification[75] and registration[76] procedures with the Ministry of Industry and Trade. Notably, this requirement also applies for foreign owners of websites using *.vn* domain names.[77]

Decree No. 52 also emphasizes transparency in e-commerce by requiring the disclosure of certain information for specific types of websites. For example, e-commerce business websites must disclose website owners' identity, information of the products and services on sale, payment and delivery methods, general terms of transaction, limitations on liability, dispute settlement mechanisms, and data security protection.[78] Furthermore, the Decree provides a broad

[68] See Anh Quân, Mua Theo Nhóm – Được Ít Mất Nhiều [Group Deals – Gain Little Lose A Lot], VN Express (Nov. 22, 2012; 12:12), http://kinhdoanh.vnexpress.net/tin-tuc/vi-mo/mua-theo-nhom-duoc-it-mat-nhieu-2724174.html

[69] See id.

[70] See The Box, Thanh toán Trực tuyến tại Việt Nam: Chưa đủ An toàn? [Online Payments in Vietnam: Not Safe Enough?], Lao Động (Oct. 19, 2012; 4:20 PM.), http://laodong.com.vn/sci-tech/thanh-toan-truc-tuyen-tai-viet-nam-chua-du-an-toan-88306.bld.

[71] See Tờ trình Chính phủ Dự thảo Nghị định về Thương mại Điện tử [Proposal to the Government regarding the Draft Decree on Electronic Commerce], Part I, available at http://www.vibonline.com.vn/Files/Download.aspx?id=2449 (last visited Apr. 20, 2014).\

[72] Nghị định về Thương mại Điện tử [Decree on E-commerce] No. 52/2013/ND-CP, issued by the Government of Vietnam on May 16, 2013 (hereinafter "Decree No. 52") (Viet.).

[73] Websites established to promote and/or sell the goods and/or services of the website owners. See Decree No. 52, Arts. 24.1 and 25.1.

[74] Websites that provide a platform for third parties to conduct e-commerce trading activities, including e-commerce platform websites, online auction websites and online promotion websites and other websites to be added by the authorities in the future. See Decree No. 52, Arts. 24.2 and 25.2.

[75] See Decree No. 52, Art. 27.1.

[76] See Decree No. 52, Arts. 36.1, 41.1, 46.1, and 55.1.

[77] See Decree No. 52, Art. 2.1(c).

[78] See Decree No. 52, Arts. 28-34.

range of prohibited acts,[79] which specifically address Muaban24 and group deal cases discussed above. Accordingly, despite the aforementioned loophole of the existing Competition Law, activities akin to illegitimate multi level marketing of services on e-commerce websites become illegal under Decree No. 52. Other steps to promote trust in e-commerce include recognizing the validity of electronic evidence,[80] clarifying the effectiveness of online contracts,[81] introducing mechanisms to rate websites' creditability, data protection policies, and to authenticate electronic contracts, [82] and providing measures to secure online payments.[83]

iii. Data Privacy Protection Concerns

The Civil Code of Vietnam addressed privacy protection issues even before the Internet was introduced in Vietnam.[84] When the government first introduced the Internet in Vietnam in 1990s, it also emphasized the need to protect personal privacy.[85] "Personal information," though defined differently in different contexts, is protected under the IT Law,[86] the Law on Electronic Transactions,[87] the Law on Consumer Protection,[88] and their implementing regulations. The collection, use, processing, transfer, and storage of personal information is subject to specific restrictions, including, inter alia, adequate disclosures, required security measures, and required consent of the data subject.

In particular, the data protection responsibilities rest on the entity that collects, processes, uses,[89] and stores[90] the data, regardless of where the data is stored. As such, the failure to obtain consent

---

[79] *See* Decree No. 52, Art 4 (including the following acts: organizing a marketing or trading network for e-commerce services, to which participants must contribute an initial amount to buy the service, and are rewarded for recruiting new participants; taking advancate of the name of e-commerce operation to illegally mobilize capital from other traders, organizations, or individuals; committing fraud to consumers on e-commerce activities, among others.

[80] *See* Decree No. 52, Arts. 9-14.

[81] *See* Decree No. 52, Arts. 15-23 (Decree No. 52 sets out clearer conditions for establishing the legal validity of e-commerce contracts. Accordingly, informational integrity of a document is established when parties agree to use certain measures such as using e-signatures certified by lawful certification organizations, or storing documents on the systems of licensed e-contract authentication organizations.)

[82] *See* Decree No. 52, Arts. 60-63 (a license from the MOIT is required in order to provide the following services: Rating the creditability of e-commerce websites; rating and certifying the policy (of a website owner) regarding the protection of personal information in e-commerce; and electronic contract authentication.)

[83] *See* Decree No. 52, Arts. 74 and 75 (owners of websites with online payment functions and suppliers of online payment services are subject to specific obligations under Decree No. 52 regarding the safety and confidentiality of online payment transactions. They may be held jointly liable for any damage caused by the illegal disclosure, amendment, reproduction, cancellation, deletion, or transfer of online payment information via the website. In addition, website owners who develop their own online payment solutions to support the online sale of their goods must apply specific measures to ensure safety and confidentiality of customer data.)

[84] Civil Code 1995 (Article 34 recognizes the right of individuals to have their privacy respected and protected by law; the collection and publication of individual privacy's information require consent). A similar principle was included in the current Civil Code No. 33/2005/QH12, adopted by the National Assembly of Vietnam on Jun. 14, 2005 (Viet.), Arts. 31 and 38.

[85] Decree No. 21, Art. 3.3.

[86] *See* Luật về Công nghệ thông tin [Law on Information Technology, No. 67/2006/QH11 adopted by the National Assembly of Vietnam on Jun. 29, 2006 ("IT Law"), Arts. 21 and 22 (Viet.).

[87] *See* Luật Giao dịch Điện tử [Law on E-Transactions], No. 51/2005/QH11 adopted by the National Assembly of Vietnam on Nov. 29, 2005, Art. 46 (Viet.).

[88] *See* Luật Bảo vệ Quyền lợi Người Tiêu dùng [Law on Protection of Consumers' Rights] No. 59/2010/QH12, adopted by the National Assembly of Vietnam on Nov. 17, 2010, Art. 6 (Viet.).

[89] Art. 21, IT Law (Viet.).

[90] Art. 22, IT Law (Viet.).

and to secure the data at any of these steps will result in liabilities for online intermediaries, including offshore service suppliers who process and host the relevant data outside Vietnam.

iv. Network Safety – Malware and Viruses

Vietnam also shares the common fear of malware and virus attacks. In order to address this fear, the government has designed regulations to control not only individual hackers' behaviors, but also those of online intermediaries.

Although spreading spam and malware is subject to criminal liability under Vietnamese law,[91] individual hackers are not easily identifiable ex-ante and the liabilities are imposed on them only when the infringements have occurred. Therefore, the government also requires online intermediaries – the limited number of government-licensed entities/the chokepoints – to apply measures to prevent the risk.[92]

For example, in order to obtain a license to provide online social networking services, suppliers must have measures to ensure information safety and security.[93] Owners of websites that have online payment functions must conduct specific practices to ensure the security and confidentiality of customers' payment transactions.[94] Furthermore, in case of "serious Internet incidents,"[95] the party facing the incident must report to appropriate members of the incident response network, including the relevant ISPs and the Vietnam Computer Emergency Response Team (VNCERT), for a coordinative solution.[96] The failure to comply with statutory information security requirements may result in administrative fines, penalties, sanctions, or civil actions.[97]

Despite all of these efforts, in May 2014 the Microsoft Security Intelligence Report announced that Vietnam was one of the top five countries with the highest rates of malware incidence.[98] Stricter liabilities against online intermediaries may thus be imposed in the near future to address this issue. In fact, the government is now introducing a draft law on information security. The proposed bill addresses information safety issues from multiple perspectives, including, inter alia, liabilities of online intermediaries in detecting, preventing and handling malwares, required

---

[91] *See* Luật Hình sự [Penal Code] No.15/1999/QH10 dated December 21, 1999, as amended under Luật Sửa đổi, Bổ sung Một số Điều của Bộ Luật Hình sự [Law Amending and Supplementing Certain Provisions of the Penal Code] No. 37/2009/QH12, Arts. 224, 225, 226a, and 226b.

[92] See Decree No. 55, Art. 18.3.

[93] Decree No. 72, Art. 23.5(dd).

[94] Decree No. 52/2013/ND-CP, Art. 74.2 (required measures include, among other things, encryption of information, access control, early detection, warning, and prevention of illegal access, and data retention and data retrieval function).

[95] Thông tư Quy định về Điều phối Các Hoạt động ứng cứu sự cố mạng Internet Việt Nam [Circular Regulating the Coordination of Responses to Internet Incidents in Vietnam] No. 27/2011/TT-BTTTT (hereinafter Circular No. 27), Art. 2 (defining "serious Internet incidents" as incidents that caused, has caused, or will potentially cause information security failures on the Internet that occur on a large scale, spread quickly, threaten serious harm to computer and Internet network systems, cause serious loss of information or which require substantial national or international resources to resolve.)

[96] *See* Circular No. 27, Art. 7.

[97] *See* IT Law, Art. 22; Civil Code, Art. 25.

[98] *See* Đỗ Nguyễn, *Việt Nam thuộc 5 Quốc gia có Tỉ lệ Nhiễm mã độc cao nhất Thế giớI* [*Vietnam within top 5 Countries with the Highest Rate of Malware Affection*], PC World VN (May 17, 2014: 18:51), http://www.pcworld.com.vn/articles/kinh-doanh/an-toan-thong-tin/201...viet-nam-thuoc-5-quoc-gia-co-ti-le-nhiem-ma-doc-cao-nhat-the-gioi/

information security breach responses, encryption technology control, information technology import control, and licensing requirements for security certification services.[99]

In short, this section assesses the liability of online intermediaries from the perspective of the concerns that Vietnam commonly shares with other jurisdictions. The current regulatory framework is designed to include online intermediaries' responsibilities to protect national security, prevent online fraud, protect the data and privacy of users, and secure the safety of the entire network. Failure to comply with such requirements will result in liability designated by law. Since these concerns remain ineffectively addressed, more stringent regulations might soon be added.

4. The Fear of the Failure to Localize the Benefit of Online Services – Domestic Call

Many countries, including Vietnam, are concerned about the fact that cross-border online businesses incurred profit locally, while leaving a small portion or no portion of such income behind domestically. So the question is how to localize the benefits of cross-border online services.

Potential answers include: support domestic service suppliers to compete against foreign suppliers; mandate or encourage a profit sharing arrangement with local entities; and subject foreign service suppliers to greater regulatory burdens, such as imposing licensing requirements, requiring localization of infrastructure, or requiring the establishment of local entities. It appears that the Vietnamese government has tried all of these, which have had a substantial effect in shaping the business environment for online intermediaries, particularly for foreign online intermediaries.

Overall, the policy has been to promote and facilitate homegrown businesses, including local online intermediaries' businesses and the business activities by foreign intermediaries that also benefit local businesses. In 2009, the Politburo of the Communist Party of Vietnam announced a campaign titled, "Vietnamese people prefer Vietnamese products."[100] In line with this campaign, the Prime Minister of Vietnam approved the National Strategy on "Transforming Vietnam into an Advanced ICT Country" in 2010.[101] "Improve the capacity and competitiveness of Vietnamese enterprises" and "develop Vietnam's ICT brand-name products and services" are two key missions of this strategy.[102] When Mr. Nguyen Bac Son became MIC Minister in 2011, the MIC implemented these missions by initiating the "Program on Promoting the development of Vietnam ICT brand-name products and services (VIBrand)."[103]

---

[99] *See* Dự thảo Luật An toàn Thông tin [Draft Law on Information Security], *available at* http://mic.gov.vn/layyknd/Trang/LUẬTANTOÀNTHÔNGTINSỐ.aspx, (*last visited* May 10, 2014)

[100] TTXVN, *Bộ Chính trị Vận động Người Việt Dùng Hàng Việt [The Politburo Campaigns for Vietnamese People to Use Vietnamese Products]* (Aug. 7, 2009, 11:09), *available at* http://dantri.com.vn/su-kien/may-bay-malaysia-mat-tich-mot-hanh-khach-dung-ho-chieu-an-cap-342309.htm (Viet.).

[101] NSCICT and MIC, White Book 2012: Information and Data on Information and communication Technology: Vietnam 2012, Information and Communications Publishing House, 15 (2011).

[102] *Id.*

[103] *Id.*

One of the first moves – allegedly driven by the Vietnamese government – that affected a foreign online intermediary was the 2009 Facebook blocking.[104] In 2010, soon after the blocking was reported, *go.vn*, a homegrown online social networking service (run by VTC Intercom, a State owned company)[105] was introduced to users. The site had the stated goal to "knock out Facebook."[106] Though *go.vn* was reported to be State sponsored, the government has since denied its involvement in the Facebook blocking.

Notably, unlike the blocking in China, which is conducted at the Internet protocol level,[107] Facebook access from Vietnam is blocked at the domain name system (DNS) level. Users can easily circumvent the blocking by using a proxy server or a virtual private network, or by changing their DNS.[108] Thus, an alternative explanation by some local experts was that the blocking might not be to afford domestic protection.[109] Rather, the main purpose was likely to draw foreign service suppliers' attention to the fact that the local authority is looking for their cooperation[110] in achieving governmental interests, including, for example, localizing certain portions of the locally generated income and obtaining convenient access to control online content accessible to local users.

In fact, despite the alleged blocking, Facebook services in Vietnam are still growing significantly.[111] Interestingly, this growth is happening in conjunction with certain local arrangements by Facebook. In January 2011, Facebook hired a Policy and Growth Manager for Vietnam.[112] In March 2011, Facebook signed the Memorandum of Understanding with a local partner, FPT Group, regarding FPT's membership to Facebook's Preferred Developer Consultant. Accordingly, the local partner will "develop specific mobile-based applications and provide advertising services for Facebook in Vietnam."[113] Most recently, Facebook appointed

---

[104] OpenNet Initiative, *Vietnam*, Aug. 7, 2012, 387-388, *available at* http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-vietnam.pdf

[105] *See* Intercom VTC, http://intecom.vtc.vn/vn/about-us (*last visited* May 10, 2014).

[106] Anh Trọng, *Go.vn Sẽ Đánh bại Facebook [Go.vn will Knock out Facebook],* Thegioididong (May 26, 2010), http://www.thegioididong.com/tin-tuc/govn-se-danh-bai-facebook-12450. *See also* James Hookway, *In Vietnam, State 'Friends' You*, Wall Street Journal (updated Oct. 4, 2010 12:01 a.m. ET), http://online.wsj.com/news/articles/SB10001424052748703305004575503561540612900?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052748703305004575503561540612900.html; Luke Allnutt, *Fearing Facebook Vietnam Launches Its Own Social Networking Site*, Radio Free Europe Radio Liberty (Oct. 5, 2010), http://www.rferl.org/content/Fearing_Facebook_Vietnam_Launches_Its_Own_SocialNetworking_Site_/2177003.html

[107] *See* H.C., *Banned, Maybe. For Some.,* The Economist (Nov. 10th, 2010, 22:40), http://www.economist.com/blogs/babbage/2010/11/facebook_vietnam.

[108] *See id. See also* OpenNet Initiative, *Vietnam*, Aug. 7, 2012, 387-388, *available at* http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-vietnam.pdf

[109] *See* Goutama Bachtiar, *Nguyen Ngoc Hieu on the State of Social Networks in Vietnam*, E27 (Nov. 30, 2011), http://e27.co/nguyen-ngoc-hieu-on-the-state-of-social-networks-in-vietnam/.

[110] *See id.*

[111] *See* Tuoitrenews, *Facebook Users in Vietnam Grow 200% in One Year*, Tuoitrenews (updated Oct. 19, 2012; 16:37), http://tuoitrenews.vn/features-news/2967/facebook-users-in-vietnam-grow-200-in-one-year. *See also* Anh-Minh Do, *Vietnam's Facebook Penetration Hits Over 70%, Adding 14 Million Users in One Year*, Techinasia (Sept. 25, 2013, 2:30 PM), http://www.techinasia.com/facebook-12-million-users-vietnam/.

[112] See the Manager's LinkedIn profile at https://www.linkedin.com/pub/tuoc-huynh/2/624/435.

[113] FPT, Facebook and PPT Announces Cooperation in Vietnam (April 4, 2011; 00:00), http://www.fpt.com.vn/en/newsroom/press_releases/2011/04/04/24492/.

T&A Ogilvy, a local partner, as its media representative in Vietnam beginning in January 2014.[114] This way of doing business by foreign service suppliers is welcomed by the government for a number of reasons. First, a part of the income incurred locally will be shared with the local partner, and thus captured domestically. Second, this local entity serves as the local contact point, bridging the foreign supplier and the local authority for liaison functions when necessary. Third, the local partner may also serve as the point of control in terms of online content management and compliance with relevant local tax obligations.

Furthermore, the Government attempted to localize the benefits earned by foreign online businesses by proposing regulations that force cross border service suppliers to enter into commercial arrangements with local partners, do business through local intermediaries,[115] establish local entities, or locate infrastructures in Vietnam.[116] As an additional effort, in April 2012, the Ministry of Finance of Vietnam officially subjected foreign suppliers generating income from online advertising and marketing to tax obligations in Vietnam.[117] With these requirements, certain parts of the income earned from the domestic market may remain within Vietnam. In addition, foreign service suppliers will be subject to the relatively equal footing with domestic suppliers in terms of establishing local infrastructure, obtaining required local licenses, and complying with other local requirements.

As such, it is not a surprise that major foreign online intermediaries such as Google and Facebook will soon be subject to more and more scrutiny from the local government. The criteria used by the local government as the basis to exercise its authority are broadly whether the relevant sites are used in Vietnam or accessed from Vietnam, as mentioned by Decree No. 72.[118] The number of Vietnamese users reaching/accessing/using the foreign site might also be a relevant criteria depending on how the regulations implementing Decree No. 72 will be crafted.[119]

All in all, Vietnamese online intermediaries will likely enjoy a facilitating environment, while foreign online intermediaries will be subject to more stringent local disciplines when generating income from Vietnam. Most of the constraints on the latter will likely be aimed at capturing a certain portion of the locally generating income inside Vietnam and facilitating censorship by the local authority.

III. Regulations Reflecting Hopes

[114] SGT, *Facebook Officially Enters Vietnam*, Vietnamnet, (Jan. 27, 2014, 13:15), http://english.vietnamnet.vn/fms/science-it/94575/facebook-officially-enters-vietnam.html.
[115] *See* Dự thảo Nghị định về Dịch vụ Công nghệ Thông tin [Draft Decree on Information Technology Services], Version 3.8, Art. 19.3, *available at* http://www.vibonline.com.vn/Duthao/1250/Nghi-dinh-ve-dich-vu-cong-nghe-thong-tin.aspx, (*last visited* Jan. 1, 2014) (Viet.).
[116] *See* Dự thảo Nghị định về Dịch vụ Công nghệ Thông tin [Draft Decree on Information Technology Services], qtcs.com, Apr. 2012, Art. 20.1, *available at* http://qtsc.com.vn/c/document_library/get_file?uuid=63cd7c9e-065c-4f06-a6a0-93ab819b7ce2&groupId=18, (*last visited* Jan. 1, 2014) (Viet.).
[117] Thông tư Hướng dẫn Thực hiện Nghĩa vụ Thuế Áp dụng Đối với Tổ chức, Cá nhân Nước ngoài Kinh doanh Tại Việt Nam hoặc có Thu nhập tại Việt Nam [Circular Guiding the Implementation of Tax Obligation Applicable to Foreign Organizations [and] Individuals Doing Businesses in Vietnam or Incurring Income from Vietnam] No. 60/2012/TT-BTC issued by the Ministry of Finance on Apr. 12, 2012, Art. 4.4 (Viet.).
[118] Decree No. 72, Art. 22.1.
[119] This is hinted from the provisions on cross borders supply of public information to large users in Vietnam under the draft version of the then adopted Decree No. 72.

The above risks and concerns, though prevalent, are only a one-sided reflection of online activities in Vietnam. Various regulations and policies adopted by the Government through different periods of time also reflect a strong hope for growth opportunities brought by the Internet. According to these policies and regulations, online intermediaries' roles are recognized in a number of fields.

1. Embracing New Opportunities for Economic Growth

As a result of the command-and-control approach in the 1990s period, Internet developments in Vietnam were constricted by the capabilities of the Vietnamese regulator. The Communist Party of Vietnam itself perceived the development of Vietnamese technology information industry in 2000 as "outdated", "low," and "far lagging behind" the level of development of other countries.[120] These disappointing outcomes and the desire to incorporate Internet growth into the wider development agenda of the country demanded that Vietnam amend its strategy. The country embraced this hope by making a leap in its economic growth through unleashing and promoting the potentials brought by the information technology ("IT") industry.[121]

The Party leaders adopted specific plans to promote IT application and development in order to serve the modernization and industrialization processes in Vietnam. The plans included measures to encourage the large scale application of IT, train human resources for the IT industry, create a supportive environment for investments in the IT sector, accelerate the construction of Internet and telecommunications infrastructure, and renovate state administration in the field.[122] This top-down instruction was implemented in three key regulations that substantially determined the roles and liabilities of online intermediaries: Decree No. 55 and its subsequent replacements,[123] the Law on Information Technology,[124] and Joint Circular No. 07. [125]

i. Decree No. 55 and Its Subsequent Replacements – Doors Opened for Online Intermediaries

Adopted in 2001, Decree No. 55 explicitly set forth the principle that "regulatory capability must keep up with developments' demand."[126] According to this principle, instead of constricting

---

[120]Chỉ thị số 58/CT-TW về Đẩy mạnh Ứng dụng và Phát triển Công nghệ Thông tin Phục vụ Sự nghiệp Công nghiệp hoá, Hiện đại hoá [Directive No. 58/TW on Promoting the Application and Development of Information Technology in Support of the Modernization and Industrialization Process], approved by the Politburo of the Central Committee of the Communist Party of Vietnam on Oct. 17, 2000, Part I (Viet.) (hereinafter "Directive No. 58").

[121] *See id.*

[122] *See id.* Part II.

[123] Nghị định 55/2001/NĐ-CP ngày 23 tháng 8 năm 2001 về Quản lý, Cung cấp và Sử dụng Dịch vụ Internet [Decree No. 55/2001/ND-CP dated August 23, 2001 regarding the Management, Provision and Use of Internet Services] (Viet.).

[124] Luật Công nghệ Thông tin của Quốc hội nước Cộng hoà Xã hội Chủ nghĩa Việt Nam số 67/2006/QH 11 ngày 29 tháng 6 năm 2006 [Law on Information Technology No. 67/2006/QH 11, adopted by the National Assembly of the Socialist Republic ò Vietnam on 29 June 2006] (Viet.) (hereinafter "IT Law").

[125]Thông tư Liên tịch Quy định Trách nhiệm Của Doanh nghiệp Cung cấp Dịch vụ Trung gian Trong việc Bảo hộ Quyền Tác giả và Quyền Liên quan trên Môi trường Mạng Internet và Mạng Viễn thông [Joint Circular on the Liabilities of Intermediary Service Suppliers in Protection of Copyrights and Related Rights on the Internet and Telecommunications Network Environment] No. 07/2012/TTLT-BTTTT-BVHTTDL, jointly issued by the Ministry of Information and Communications and the Ministry of Culture, Sport, and Tourism on Jun. 19, 2012 (hereinafter "Joint Circular No. 07") (Viet.).

[126] Decree No. 55, Art. 3.1.

Internet developments to the authority's regulatory capability (as adopted during the 1991-2000 period), Internet developments are the goals that regulatory measures serve to achieve.

The Decree also outlined the goal of "developing diversified Internet services at high quality and reasonable price in order to serve the nation's industrialization and modernization progress."[127] In particular, the Decree explicitly acknowledged the roles of Internet services in popularizing government policies to the public and facilitating the advertisements of private goods and services on the Internet.[128]

While IXPs remained wholly or predominantly owned by the government, ISPs were open for all types of ownership. Notably, Decree No. 55 introduced a new category of service suppliers — "Online Service Providers" (OSP), which are enterprises that use the Internet to provide application services such as telecommunications, information, culture, commerce, banking, finance, healthcare, education, and technical assistance to users.[129] Unlike IXPs, ISPs, and ICPs, which are subject to licensing requirements directly provided under Decree No. 55, OSPs are only subject to the regulations of specific State management agencies (if any).[130] As one of the measures to promote the application of the Internet, the Decree explicitly entitled users to use Internet application services of both domestic and foreign OSPs, except for the services whose use is prohibited or not yet permitted.[131]

Decree No. 97,[132] which replaced Decree No. 55 in 2008, reiterated the spirit mentioned under Decree No. 55. Furthermore, despite some additional constraints as analyzed in the previous section, Decree No. 72,[133] which recently replaced Decree No. 97, continues to emphasize the government's policies of, among other things:

"Promoting the use of Internet in all economic and social activities, especially in education and training, health care, and scientific and technological research in order to raise productivity, create jobs and improve the quality of life; Encouraging the development of contents and applications in Vietnamese to serve the Vietnamese community on the Internet; [and] Intensifying the upload of healthy and useful information to the Internet."[134]

ii. IT Law – Promoting IT Development and Application

The IT Law similarly promotes the application and development of information technology in various fields, including governmental operation and commerce. The words "encourage," "facilitate", and "prioritize" were mentioned multiple times in the Law.

In line with this encouraging atmosphere, the Law explicitly exempts online intermediaries from liabilities in certain circumstances. For example, entities transmitting digital information are not

[127] Decree No. 55, Art. 3.2.
[128] *See id.*, Art. 5.
[129] *See id.*, Arts. 12.3, 13.3.
[130] *See id.*, Art. 36.
[131] *See id.*, Art. 22.2
[132] Nghị định của Chính phủ số 97/2008/NĐ-CP ngày 28 tháng 8 năm 2008 về Quản lý, Cung cấp, Sử dụng Dịch vụ Internet và Thông tin Điện tử trên Internet [Decree No. 97/2008/ND-CP of the Government dated August 28, 2008 on Management, Provision, and Use of Internet Services and Electronic Information on the Internet] (Viet.)
[133] Nghị định Quản lý, Cung cấp, Sử dụng Dịch vụ Internet và Thông tin trên mạng [Decree on Management, Provision, and Use of Internet Services and Online Information] No. 72/2013/ND-CP dated July 15, 2013 (Viet.)
[134] Decree No. 72, Arts. 4.1 and 4.2.

liable for the information content unless they self-initiate, select or modify the content, or select the recipients of the information.[135] Similarly, those who temporarily store digital information are not liable for the information content unless they modify the content, illegally collect data, disclose information, or fail to comply with regulations on information accession or update.[136]

The Law also explicitly provides that, unless otherwise required by the competent authorities, entities applying information technologies are not responsible for tracking or monitoring digital information of third parties, or investigating infringing acts of third parities while transmitting or storing their information.[137]

iii. Joint Circular No. 07 – Online Intermediaries' Liabilities in Copyrights Protection

In implementing the IT Law, Joint Circular No. 07[138] clarifies the liabilities of intermediary service suppliers in protecting copyrights and related rights on the Internet and telecommunications network environment.

Accordingly, telecommunications service suppliers, Internet service suppliers, providers of online social network services, providers of information search services, and companies leasing digital information storage space are directly liable for infringing content only in limited circumstances.[139] The circumstances include when the service suppliers initiate the posting, transmit or provide of the infringing content over the Internet or telecommunications network, modify or copy the infringing content, deliberately circumvent technology measures applied by right owners to protect copyrights or related rights, or operate as the secondary distributors of the infringing content.[140]

Though there are criticisms[141] as to the government's failure to adopt a "safe harbor" regime, which enables notice-and-take down mechanisms resembling that under the DMCA in the United States,[142] these regulations illustrate the Government's acknowledgement of the need to exempt online intermediaries from certain liability, as well as the role of online intermediaries in protecting copyrights and related rights.

2. Turning Vietnam Into a Nation With a Strong IT Industry and With a Knowledge-Based Economy

i. Online Intermediaries as Supporters of Business Development

---

[135] IT Law, Art. 16.4.
[136] IT Law, Art. 17.2.
[137] IT Law, Art. 20.2.
[138]Thông tư Liên tịch Quy định Trách nhiệm Của Doanh nghiệp Cung cấp Dịch vụ Trung gian Trong việc Bảo hộ Quyền Tác giả và Quyền Liên quan trên Môi trường Mạng Internet và Mạng Viễn thông [Joint Circular on the Liabilities of Intermediary Service Suppliers in Protection of Copyrights and Related Rights on the Internet and Telecommunications Network Environment] No. 07/2012/TTLT-BTTTT-BVHTTDL, jointly issued by the Ministry of Information and Communications and the Ministry of Culture, Sport, and Tourism on Jun. 19, 2012 (hereinafter "Joint Circular No. 07") (Viet.).
[139] *See* Joint Circular No. 07, Arts. 3.1 and 5.
[140] Joint Circular No. 07, Art. 5. 5.
[141] *See* Baker & McKenzie Vietnam, *Intermediary Service Supplier's Copyright Liabilities on the Internet*, July 2012,
[142] Online Copyright Infringement Liability Limitation Act, as part of the Digital Millennium Copyright Act, 17 U.S. Code §512.

In 2010, the Prime Minister of Vietnam approved a project named "Soon Turning Vietnam into a Strong Nation in Information Technology and Communications."[143]

Accordingly, the government continues to focus on training IT human resources to serve not only domestic demand, but also for labor export.[144] Investments in infrastructure to support the application and development of information technology are also prioritized. Furthermore, the government "encourages enterprises to develop IT technologies for application in daily life and in governmental operation," and "provide information and online services to support the people and businesses on the basis of cooperation between the Government and the enterprises."[145]

The authority sees the application of information technology in society as a means to "improve people's knowledge."[146] The targets by 2015 are to provide basic governmental services online, apply information technology in management, operation, and business operation of 80% enterprises and social organizations, universalize IT application in the education and healthcare systems, and enhance the application of IT in national defense and security.[147]

As such, this Project officially recognizes the role of online intermediaries as information providers and as supporters of business development. The strategy under this Project is in line with the broader agenda of Vietnam to industrialize and modernize the country by improving the quality of the labor force, such that the economy will become "knowledge based,"[148] rather than manual (or cheap labor) based.

ii. Opportunities Brought by E-Commerce

Vietnam also recognizes the opportunities brought by e-commerce. In 2010, the Prime Minister of Vietnam approved a number of solutions for "making e-commerce a popular practice at the advanced level in the ASEAN region, contributing to enhance the competitiveness of enterprise and the nation, and promoting the country's industrialization and modernization progress."[149] The plan contains detailed targets for digitalizing a majority of business activities and governmental services by 2015, including the targeted percentile of enterprises embracing electronic means for their business operation.[150]

---

[143] Quyết định Phê duyệt Đề án "Đưa Việt Nam Sớm Trở thành Nước mạnh về Công nghệ Thông tin Và Truyền thông" [Decision Approving the Project of "Soon Turning Vietnam into a Strong Nation in Information Technology and Communications"] No. 1755/QD-TTg, adopted by the Prime Minister of Vietnam on Sept. 22, 2010 (Viet.).

[144] Quyết định Phê duyệt Kế hoạch Tổng thể Phát triển Nguồn Nhân lực Công nghệ Thông tin Đến năm 2015, Định hướng đến Năm 2020 [Decision Approving the General Plan in Developing the Information Technology Human Resources by 2015 [and] Orientation Toward 2020] No. 698/QD-TTg adopted by the Prime Minister on June 1, 2009. This Decision was then incorporated into an annex of Decision No. 1755.

[145] Decision No. 1755, Part IV, Section 5(a).

[146] *Id.*, Part III, Section 4.

[147] *See* Decision No. 1755, Part I, Section 2(dd).

[148] Chỉ thị Về Định hướng Phát triển Công nghệ Thông tin và Truyền thông Việt Nam Giai đoạn 2011-2020 (gọi tắt là "Chiến lược Cất cánh") [Directive on Orientation Strategy for the Development of Information Technology and Communications for the 2011-2020 period (abbreviated as the "Take Off Strategy")] No. 07/CT-BBCVT, issued by the Ministry of Post and Telematics on Jul. 7, 2007, Section 2 (Viet.).

[149] Quyết định Phê duyệt Kế hoạch Tổng thể Phát triển Thương mại Điện tử Giai đoạn 2011-2015 [Decision Approving the General Plan for the Development of Electronic Commerce in the 2011-2015 Period] No. 1073/QD-TTg, adopted by the Prime Minister of Vietnam on Jul. 12, 2010, Art. 1, Part A, Section I (Viet.).

[150] *See id*, Art.1, Part A, Section II.

In 2012, the Executive Committee of the Communist Party of Vietnam set "quickly developing the e-commerce system" as the key focus of commercial infrastructure development efforts.[151] The Government identifies "studying, constructing, and applying appropriate mechanisms to encourage the development of electronic commerce" as one of the main approaches for the socio-economic development of the year 2012.[152]

The Ministry of Industry and Trade, the State agency responsible for e-commerce management, has also tasked itself with strongly applying e-commerce and diversifying e-commerce activities, promoting paperless transactions to facilitate commercial activities, and quickly applying e-commerce to create modern distribution channels.[153]

iii. Booming of Internet Activities

The above policies and regulations explain the boom of Internet use and application in Vietnam. Notably, Vietnam has been ranked among the nations with the fastest annual growth rates of Internet users.[154] By June 30, 2012, the country had over 31 million Internet users, accounting for over 33% of its population.[155]

Businesses such as airlines, travel agencies, and hotels embrace online platforms are the key channel for their sales.[156] The national tourism promotion program for the 2013-2020 period identifies social networks, smart phones, and the Internet as the prioritized channels for tourism promotion.[157] Experts labeled the digital advertising market in Vietnam as "booming" in 2013, with an estimated turnover of $32 million and this is expected to reach $45 million by 2015.[158]

---

[151] Nghị quyết Hội nghị Lần Thứ Tư Ban Chấp hành Trung ương Khoá XI Về Xây dựng Hệ thống Kết cấu Hạ tầng Đồng bộ Nhằm đưa Nước ta Cơ bản Trở thành Nước Công nghiệp Theo hướng Hiện đại vào Năm 2020 [Resolution at the Fourth Conference within Session XI of the Executive Committee Regarding the Construction of a Harmonized Infrastructure System for Bring Vietnam to Basically Become an Industrialized Nation with Modern Orientation by 2020] No. 13-NQ/TW adopted by the Executive Committee on Jan. 6, 2012, (Viet.).

[152] Nghị quyết Về Những Giải pháp Chủ yếu Chỉ đạo Điều hành Thực hiện Kế hoạch Phát triển Kinh tế - Xã hội và Dự toán Ngân sách Nhà nước Năm 2012 [Resolution on the Main Solutions in Directing and Managing the Implementation of Socio-Economic Development Plan and Estimated State Budget in 2012] No. 01/NQ-CP, adopted by the Government of Vietnam on Jan. 3, 2012, First Part, Section I, Point 3, third bullet point (Viet.).

[153] *See* Tờ trình Chính phủ Dự thảo Nghị định về Thương mại Điện tử [Proposal to the Government regarding the Draft Decree on Electronic Commerce], Part II, *available at* http://www.vibonline.com.vn/Files/Download.aspx?id=2449 (*last visited* Apr. 20, 2014).

[154] *See* National Steering Committee on ICT (NSCICT) and Ministry of Information and Communications (MIC), White Book 2013: Vietnam information and communication technology, Information and Communications Publishing House, (2013), at 22.

[155] Internet World Stats, Vietnam, http://www.Internetworldstats.com/asia.htm#vn (*last visited* Apr. 20, 2014).

[156] *See* Tờ trình Chính phủ Dự thảo Nghị định về Thương mại Điện tử [Proposal to the Government regarding the Draft Decree on Electronic Commerce], Part I, *available at* http://www.vibonline.com.vn/Files/Download.aspx?id=2449 (*last visited* Apr. 20, 2014).

[157] *See* Quyết định Phê duyệt Chương trình Xúc tiến Du lịch Quốc gia Giai đoạn 2013-2020 [Decision Approving the National Tourism Promotion Program for the 2013-2020 Period] No. 2151/QD-TTg, issued by the Prime Minister of Vietnam on Nov. 11, 2013, Art. 1.2(c) (Viet.). *See also* SGT, *Vietnam to Use Social Networks, Internet to Promote Tourism*, Vietnamnet (Nov. 26, 2013; 13:00), http://english.vietnamnet.vn/fms/travel/89654/vietnam-to-use-social-networks--Internet-to-promote-tourism.html.

[158] *See* K. Chi, *Digital Ad Market Booming in Vietnam*, Vietnamnet (Dec. 3, 2013), http://english.vietnamnet.vn/fms/business/90538/digital-ad-market-booming-in-vietnam.html

According to the Chairman of the Vietnam Internet Association, "enterprises are making the shift to online marketing and advertising."[159] Experts also predict a "strong growth" in e-commerce in Vietnam in the years to come.[160] Some expect that the total revenues of Internet services and content to be VND 100 trillion (approximately USD 47 billion) by 2018.[161]

All in all, in parallel with the constraints originating from the fears analyzed in the previous section, Vietnam also embraces the opportunities brought by online intermediaries to the country's business development. This gives room for the expansion of online intermediaries' business activities in Vietnam, and implies a broader responsibility of online intermediaries regarding their contribution to the development of the local economy.

III. Conclusion

The above analysis illustrates both the fears and the hopes related to online activities in Vietnam. The policies and regulations by the Vietnamese authority correspond to and address these hopes and fears. Thus far, the fears seem to be dominant in comparison to the hopes. Besides the common fears regarding national security, prevention of fraud, data and privacy protection, and network security, fears also originate from the specific political and economic conditions of Vietnam.

The fears involving the protection of the current regime's ideology and the demand for localizing the benefits incurred from online activities dictate the stringent liabilities on online intermediaries. At the same time, online intermediaries will likely have room for strong developments in Vietnam due to the hope of the government to embrace new opportunities for economic growth, and its desire to turn Vietnam into a nation with a strong IT industry and with a knowledge-based economy. As a result, online intermediaries' may have to exercise their roles in accordance with specific requests from the authorities in order to avoid liabilities. Though the liabilities of offshore online intermediaries that provide services to Vietnamese users on a cross-border basis currently remain ambiguous in certain areas, the participation of these intermediaries in the Vietnamese market may also demand similar cooperation with the local Government to address relevant fears. Having said this, it is worth noting that the aggressiveness of government requirements may potentially be restrained by specific commitments of Vietnam under applicable international arrangements.

[159] VNA, *E-Commerce Enjoys Strong Growth*, Vietnamplus (Dec. 8, 2013), http://en.vietnamplus.vn/Home/Ecommerce-enjoys-strong-growth/201312/43116.vnplus.
[160] *Id.*
[161] *See id.*