September 2014

Law of the Intermediated Information Exchange

Jacqueline D. Lipton
Case Western Reserve University School of Law, jdl14@case.edu

LAW OF THE INTERMEDIATED INFORMATION EXCHANGE

Jacqueline D. Lipton[*]

Abstract

When Wikipedia, Google and other online service providers staged a 'blackout protest' against the Stop Online Piracy Act in January 2012, their actions inadvertently emphasized a fundamental truth that is often missed about the nature of cyberlaw. In attempts to address what is unique about the field, commentators have failed to appreciate that the field could – and should – be reconceptualized as a law of the global intermediated information exchange. Such a conception would provide a set of organizing principles that are lacking in existing scholarship. Nothing happens online that does not involve one or more intermediaries – the service providers who facilitate all digital commerce and communication by providing the hardware and software through which all interactions take place. This Article advocates a fundamental shift in the nature of cyberspace scholarship towards a law of the 'intermediated information exchange.' The author explains the benefits of such an approach in developing a more predictable and cohesive body of legal principles to govern cyberspace interactions.

[*] Professor of Law and Associate Dean for Faculty Development and Research, Case Western Reserve University School of Law, 11075 East Boulevard, Cleveland, Ohio, 44106 (Email: JDL14@case.edu). The author would like to thank Professor Joel Reidenberg, Ms Jamela Debelak, and participants at the Law and Information Society Informational Workshop at Fordham Law School (hosted by the Center on Law and Information Policy) on September 16, 2011 for generous support in workshopping of an earlier draft of this paper. Particular thanks to Professor Derek Bambauer, Professor Steven Bellovin, Professor Gaia Bernstein, Professor Irina Manta, Professor Ira Bloom, Professor Margaret Chon, Professor Leah Grinvald, Mr Jordan Kovnot, Professor Ed Lee, Professor Jessica Litman, Professor David Post, Professor Susan Scafidi, Professor Olivier Sylvain, Professor Jane Yakowitz, Dean Lawrence Mitchell, Professor Nancy Kim, Professor Sharona Hoffman, Professor James Grimmleman, and Professor Cassandra Robertson for comments on earlier drafts of this article. All mistakes and omissions are, of course, my own.

INTRODUCTION

The January 2012 'blackout protest' against the Stop Online Piracy Act (SOPA) mounted by Wikipedia, Google, and other online service providers[1] brings into sharp relief what is unique about cyberlaw as a legal field. The current SOPA bill[2] is the most recent example of the ongoing battle between market players and lawmakers in attempting to delineate the boundaries of legal responsibility for wrongful online conduct. As a longtime casebook author and teacher of cyberlaw, I have struggled, along with many of my colleagues, to provide a cohesive theoretical framework for the study of the subject. In a typical law school course, professors usually start out with general questions relating to the nature of cyberspace and the impact of the technology on the development of legal regulation. Invariably this leads to a discussion of Judge Easterbrook's infamous dismissal of cyberlaw as nothing more than a cyber 'law of the horse' that fails to illuminate the entire law in a meaningful way because it has no unifying features.[3]

What is easy to miss about cyberlaw – and what the battle over SOPA brings to the forefront of the debates – is that the field is, in reality, the law of the intermediated information exchange. All online interactions – social, commercial, academic, artistic – are exchanges of information facilitated by one or more third party intermediaries. These third parties include search engines, payments systems, Internet service providers (ISPs), gaming platforms, social network operators, domain name registrars, and web hosting services. Nothing can happen online that does not involve one or more of these actors. Moreover, it is the struggle to address the legal role of these actors with respect to online wrongs that creates the law and policy challenges that are unique to cyberspace.

The law of cyberspace is in reality the law of the intermediated information exchange transacted on a global stage. This realization suggests that the dual foci of cyberspace law should be: (a) the role and

---

[1] For discussion of the protest, see, for example, Amy Goodman, *The SOPA Blackout Protest Makes History*, The Guardian, January 18, 2012 (available at http://www.guardian.co.uk/commentisfree/cifamerica/2012/jan/18/sopa-blackout-protest-makes-history, last viewed on February 8, 2012).

[2] H.R. 3261 1H (112 Cong.), text available at: http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.3261:, last viewed on February 8, 2012).

[3] Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U CHI LEGAL F 207, 207-208 (1996).

regulation of online intermediaries; and, (b) associated jurisdictional challenges. This Article sets out a new theoretical framework for cyberlaw that is more cohesive and principled than the current piecemeal approaches found in most casebooks.[4]

Part I critiques existing approaches to cyberlaw and explains why current paradigms fail to serve the needs of the field as it has developed over the last ten to fifteen years. The author suggests that past scholarship has missed the mark in failing to focus on what is truly unique about cyberspace – its nature as a global intermediated communications medium. Part II suggests novel ways for re-organizing the field to focus on the role of online intermediaries in a global communications environment. Part III examines jurisdictional challenges that are unique to cyberspace and suggests ways in which they might be appropriately addressed within a reconceptualized cyberlaw field. Part IV concludes by drawing together the issues raised in Parts II and III in order to formulate a new approach to the field with significantly more internal cohesion than has been the case in the past.

I. CURRENT CONCEPTIONS OF CYBERLAW

Despite the resilience of cyberlaw as a staple in today's law school curricula, no one has yet accurately explained the nature of the field. It has been in the face of uncertainties surrounding its boundaries that casebook writers (myself included) began to organize the debate around the infamous 'law of the horse' categorization of cyberspace law offered by Judge Frank Easterbrook in 1996,[5] and the response to Easterbrook penned soon after by eminent cyberspace scholar, Professor Lawrence Lessig.[6]

In remarks prepared following an invitation to comment on property law in cyberspace in the 1990s, Judge Easterbrook likened cyberspace law to a cyber "law of the horse". He noted that courses involving the cross-sterilization of several fields, such as law and technology, tended to offer the worst of both worlds.[7] They would be doomed to be taught by professors who "knew little about either field".[8] He further opined that the most effective way to learn laws as they might apply to specialized

---

[4] See discussion in Part I, *infra*.

[5] Easterbrook, *supra* note 3.

[6] Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999).

[7] Easterbrook, *supra* note 3, at 207.

[8] *Id.*

endeavors is to study rules of general application.[9] Otherwise, any new field that emerged would lack unifying principles that might illuminate anything meaningful about the law more generally.[10]

In his oft-cited response to Easterbrook, Professor Lawrence Lessig claimed that cyberlaw did, in fact, illuminate the entire law, although not in the way described by Easterbrook.[11] Lessig acknowledged that cyberlaw might be conceived as a series of disconnected tort, contract, and intellectual property problems as a matter of substance.[12] However, he noted that: "there is an important general point that comes from thinking in particular about how law and cyberspace connect."[13] This general point was not about the *substance* of the law as it might be applied in cyberspace, but rather about the *limits on law as a regulator.*[14]

Lessig utilized this insight as a springboard for his well-known work on the application of multiple regulatory modalities to cyberspace. These modalities include law, social norms, markets, and system architecture.[15] Lessig's work has emphasized the significance of system architecture, or software code, as the key regulatory modality for cyberspace. He has noted that online behavior can be more or less completely and almost perfectly regulated by software code to an extent that could never be paralleled by legal rules, which are often poorly understood and imperfectly enforced.[16]

---

[9] *Id.*

[10] *Id*., at 207-8.

[11] Lessig, *supra* note 6.

[12] *Id*, at 502 ("Courses in law school, Easterbrook argued, 'should be limited to subjects that could illuminate the entire law.' '[T]he best way to learn the law applicable to specialized endeavors,' he argued, 'is to study general rules.' This 'the law of cyberspace,' conceived of as torts in cyberspace, contracts in cyberspace, property in cyberspace, etc., was not.")

[13] *Id.*

[14] *Id.*

[15] *Id.*, at 503-504 (identifying these four modalities of regulation in both physical world and cyberspace contexts).

[16] *Id*., at 514 ("I argued that whether cyberspace can be regulated is not a function of Nature. It depends, instead, upon its architecture, or its code. Its regulability, that is, is a function of its design."); Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 555 (1998) ("This Article argues, in essence, that the set of rules for information flows imposed by technology and communication networks form a 'Lex Informatica' that policymakers must understand, consciously recognize, and encourage"); 556 ("policymakers can and should look to Lex Informatica as a useful extra-legal instrument that may be used to achieve objectives that otherwise challenge conventional laws and attempts by governments to regulate across jurisdictional lines").

The tendency to focus cyberlaw scholarship on the Easterbrook-Lessig debate in subsequent years has become problematic for two reasons. The first is that it effectively freezes the debate within conceptions of the Internet as it existed in the early to mid 1990s. Little attempt has been made by subsequent scholars to move the debate towards more modern conceptions of the Internet. In other words, the debate as framed today tends to lack the benefit of hindsight, the ability to look at what the Internet has become and what unique legal issues have arisen in cyberspace since Easterbrook and Lessig presented their early comments.

The second drawback of relying on the Easterbrook-Lessig debate as an organizing focus for the modern study of cyberlaw is that such an approach tends to polarize scholars into two camps – those who believe that cyberlaw is not really a field of law at all, and those who believe that cyberlaw is a field that involves the complex interplay of multiple regulatory modalities of which software code is perhaps the most significant.[17] While aspects of each point of view are undoubtedly correct, scholars have tended to avoid developing alternate explanations for cyberspace law.[18]

Paradoxically, in the meantime, other important areas of cyberlaw scholarship have evolved, including a body of literature about the extent to which spatial metaphors derived from the physical world could – or should – be meaningfully applied to cyberspace.[19] Another ongoing debate has focused on the regulatory competence of domestic governments over the Internet.[20] Important as these bodies of scholarship have unquestionably become, they do not answer the most foundational questions about the

---

[17] See *supra* note 16.

[18] There have been some exceptions to this general trend. See, for example, Raymond Ku, *A Brave New Cyberworld?* 22 T. JEFFERSON L. REV. 125 (2000); Ira Nathenson, *Best Practices for the Law of the Horse: Teaching Cyberlaw and Illuminating Law Through Online Simulations*, 28 SANTA CLARA COMPUTER AND HIGH TECH. L. J. ___ (forthcoming, 2012).

[19] See, for example, John Perry Barlow, Cyberspace Declaration of Independence (1996) (available at https://projects.eff.org/~barlow/Declaration-Final.html, last viewed on August 1, 2011); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439 (2003); Mark Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521 (2003); Jacqueline Lipton, *Mixed Metaphors in Cyberspace: Property in Information and Information Systems*, 35 U. CHI. L. J. 235 (2003); Julie Cohen, *Cyberspace As/And Space*, 107 COLUM. L. REV. 210 (2007).

[20] See, for example, JACK GOLDSMITH and TIM WU, WHO CONTROLS THE INTERNET: ILLUSIONS OF A BORDERLESS WORLD (2008) (arguing that national governments can and do regulate cyberspace effectively); DAVID POST, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STUDY OF CYBERSPACE (2009) (arguing against domestic governments regulating cyberspace).

nature and contours of cyberlaw as a legal field.

This Article argues that scholars can and should revisit the debate about the nature of cyberlaw with the benefit of hindsight, the ability to examine pertinent legal developments, and marketplace advances, since the early Easterbrook-Lessig debates. Common unifying threads for the field have emerged if one is prepared to tease them out. They arise from the fact that the Internet is a *global communications forum* above all else and that all Internet interaction must be facilitated by *third party intermediaries*. Thus, a conception of cyberlaw that focuses on its *global nature* and on the role of these *intermediaries* will provide the unified framework that Easterbrook felt was lacking in 1996.

Additionally, while Lessig was undoubtedly correct in conceiving of cyberlaw as involving an interaction between various online regulatory modalities – including laws, social norms, market forces, and software code[21] – there is still a need within the literature for a conception of cyberlaw that focuses on the *legal* aspect of this equation. In the real world, law always interacts with other modes of regulation. Our behavior in the tangible universe is constrained as much by physical fences and walls and social mores as it is by legal rules.[22] This is no different in cyberspace, other than the fact that the precise content of the norms and the nature of the system constraints may vary online from those we face in the real world.

It is imperative that scholars engage with Internet *law* as a specific endeavor outside the interaction of the law with other modes of online regulation. Lessig and others may well be correct in suggesting that system architecture is a more effective regulator of online behavior than legal rules.[23] But that is no reason not to develop the legal rules appropriately within the context of a more cohesive theoretical framework. In the real world, prison bars and guards with guns provide more effective constraints on the behavior of convicted criminals than sentencing laws. But that is no

---

[21] Lessig, *supra* note 6, at 507-8.

[22] *Id.* ("And finally, there is a fourth feature of real space that regulates behavior – 'architecture.' By 'architecture' I mean the physical world as we find it, even if 'as we find it' is simply how it has already been made. That a highway divides two neighborhoods limits the extent to which the neighborhoods integrate. That a town has a square, easily accessible with a diversity of shops, increases the integration of residents in that town. That Paris has large boulevards limits the ability of revolutionaries to protest. That the Constitutional Court in Germany is in Karlsruhe, while the capital is in Berlin, limits the influence of one branch of government over the other. These constraints function in a way that shapes behavior. In this way, they too regulate.")

[23] See *supra* note 16.

reason not to maintain a body of sentencing law.

The aim of this article is to renew and refocus debates on the nature of cyberlaw. The key features of the Internet for the purposes of this discussion are: (a) all online conduct involves information exchange as opposed to physical contact;[24] (b) all online communications are facilitated by one or more Internet intermediaries such as ISPs, search engines, gaming platforms, and payments systems; and, (c) most online interaction has at least the potential for global reach.

No one can interact online without contracting with an ISP. The Internet experience is only meaningful in terms of interactions, all of which must be facilitated by intermediaries such as Facebook,[25] Flickr,[26] MySpace,[27] Shutterfly,[28] Amazon,[29] and Google[30]. Internet intermediaries appear at many points within the online experience, and they are necessary to enable all online experiences.

The fact that everything on the Internet may be described as an intermediated information exchange ultimately sets the parameters for cyberlaw, and sets cyberlaw apart as a distinct legal field. Understanding cyberlaw means understanding the nature and regulation of an information exchange involving more than just the originator and the recipient of a communication. One must further consider the impact of the global nature of the Internet on all of these issues. As most Internet disputes have the potential to raise jurisdictional concerns, there is a high risk within

---

[24] The information exchange is made possible by hardware and by electrons passing through cables, but my suggested focus for cyberlaw is on the informational qualities of the exchange rather than the hardware. A good discussion of confusion between hardware and content-based analyses of the Internet that plagued early discussions of Internet law can be found in: Orin Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357 (2003).

[25] Facebook is a popular online social networking service. See www.facebook.com, last viewed on August 1, 2011.

[26] Flickr is an online photo-sharing service. See www.flickr.com, last viewed on August 1, 2011.

[27] MySpace is a social networking service and forum for sharing popular culture. See www.myspace.com, last viewed on August 1, 2011.

[28] Shutterfly is an electronic business engaging in printing photographs and associated merchandise for customers as well as providing platforms for sharing photographs. See www.shutterfly.com, last viewed on August 1, 2011.

[29] Amazon.com is an iconic early experiment in electronic commerce that started as a book and music retailer online and has grown to expand into various different kinds of online marketplaces. See www.amazon.com, last viewed on August 1, 2011.

[30] Google is probably the world's leading search engine. See www.google.com, last viewed on August 1, 2011.

cyberlaw that the prominence of jurisdictional issues may detract from the development of substantive legal rules. It is to these issues that the remainder of this discussion now turns.

II. INTERNET INTERMEDIARIES

A. Defining Online Intermediaries

For the purposes of this discussion, Internet intermediaries include any service provider that enables online interaction through either paid subscription or general availability to the public.[31] These intermediaries will all maintain distinct business models. They may make their money through subscription fees, through collecting user information and marketing it to other parties, through advertising, or through a combination of these approaches. However, the common feature is that they enable and facilitate online communications in many spheres – commercial, personal, social, artistic, academic etc.

Without intermediaries, no one could go online or do much of anything by way of online activity. Intermediaries thus play a powerful and important role. Where one intermediary holds a dominant position in a relevant niche – such as Google for online searching or Facebook for social networking – the power of that intermediary may warrant significant scrutiny.[32]

Identifying the role of Internet intermediaries in terms of their legal responsibilities is in many ways the foundational challenge of cyberlaw. The legal challenges that are unique to cyberspace law and that differentiate cyberlaw from other fields arise from the ways in which, and extent to which, legislatures and courts are prepared to impose liability on intermediaries for online conduct initiated by others.[33] The focal position of

---

[31] Jacqueline Lipton, *"We, the Paparazzi": Developing a Privacy Paradigm for Digital Video*, 95 IOWA L REV 919, 931-932 (2010) (distinguishing between closed networks that require individual membership and open networks which are generally accessible to the public).

[32] See, for example, JANET LOWE, GOOGLE SPEAKS: SECRETS OF THE WORLD'S GREATEST BILLIONAIRE ENTREPRENEURS, SERGEY BRIN AND LARRY PAGE, 10 (2009) (noting that as Google gained market share and power, it also gained negative publicity for becoming too powerful); Facebook has attracted much criticism for its lack of privacy protections for users. See, for example, Rory Cellan-Jones, *Facebook Faces Criticism on Privacy Change*, BBC News, Dec 10, 2009 (available at http://news.bbc.co.uk/2/hi/8405334.stm, last viewed on August 1, 2011).

[33] See discussion in Part II.C, *infra*.

intermediaries within cyberlaw is further emphasized by the power these intermediaries can wield over the user experience thorugh their ability to control the software code that enables online interaction and their ability to monitor online conduct.

Intermediaries can control the user experience by regulating initial user access through passwords and other encryption technologies. Additionally, they can control and monitor all aspects of the user experience on their platforms by manipulating the underlying software code.[34] An avatar in Second Life can only be – and do - what the software will support. Initially, Second Life did not provide skin colors for avatars outside the Caucasian range. The game now supports the creation of additional tones – or "skins"[35] - for participants who want their avatars to appear as African American, Native American, or Asian, for example. But presumably if Linden Laboratories, the creators of Second Life, objected to the creation of different skin colors, they could disable features of the software that allow users to create such skins.

Intermediaries are the most effective choke points for enforcing desired norms of behavior online either through their own policies or through the enforcement of legal rules, or a combination of both.[36] Judicial orders directed at intermediaries are much more likely to result in effective relief to plaintiffs than orders against often globally dispersed, impecunious private actors with limited to no control over the flow of harmful information once it has been initially uploaded to a website.[37] An order requiring a major online intermediary – such as Facebook or YouTube – to remove defamatory or copyright infringing content, for example, is much more likely to be effective in practice than an attempt to seek out any number of private individuals in various jurisdictions who may be responsible for posting the infringing content in the first place.[38]

---

[34] See *supra* note 16.

[35] See http://secondlife.com/destinations/fashion/skins, last viewed on August 1, 2011 (demonstrating ways to customize skin and body shapes in Second Life).

[36] Lipton, *supra* note 31, at 936-941 (evaluating rules of conduct promulgated by online service providers and limitations to their effective enforcement).

[37] Jacqueline Lipton, *Combating Cyber-Victimization*, 26 BERKELEY TECH. L. J. 1103, 1139 (2011) ("Laws per se suffer from difficulties of identifying an anonymous or pseudonymous defendant and having effective jurisdiction reach over the defendant…. Even if plaintiffs can identify their defendants – which may require an expensive and time consuming court order – they are often judgment-proof.")

[38] A court order against an intermediary will not be a perfect solution given the tendency for information to jump from website to website online, but it will be more effective than an order against one or more private individuals.

B. Direct Versus Indirect Liability for Internet Intermediaries

The power and prominence of intermediaries underscore the importance of regulating these entities as a focal point for cyberlaw. By the same token, it is important that intermediaries, particularly those providing novel services, are not over-regulated to the point that online innovation is chilled. Lawmakers are routinely faced with difficult questions involving the regulation of powerful, and often extremely innovative, intermediaries. These questions include determining when an intermediary should be held liable for harmful online conduct instigated by another. Increasingly, Congress has drafted laws aimed specifically at the role of online intermediaries in an attempt to create clearer *ex ante* guidelines to balance technological innovation against the need to protect existing legal rights – such as copyright, trademarks, personal reputations etc. Obvious examples include the ISP safe harbor provisions in the copyright act[39] and the Communications Decency Act respectively,[40] as well as the contentious provisions of SOPA.[41]

The problem with many current cyberlaw texts is that questions of intermediary liability are scattered throughout chapters focusing on specific heads of tortious liability – copyright, trademark, defamation etc. This organization tends to discourage a focus on the central question involving the rights and obligations of intermediaries across discrete subject matter areas. Questions about intermediary liability for copyright infringement will be found in a textbook chapter on copyright law, while intermediary liability for defamation and privacy will typically be discussed in a free speech, privacy, or general tort chapter. It would make much more sense for discussions of intermediary liability to be considered together across all relevant fields of law – copyright, trademark, defamation, privacy, bullying, harassment etc. Taking this approach, important synergies inherent in the role of intermediaries could be drawn out, and more consistent and predictable legal rules developed.

For example, one question that plagues cyberlaw is the increasing difficulty inherent in ascertaining when an intermediary should be held primarily, as opposed to secondarily, liable for an online wrong. Where a wrong is committed in the physical world – such as theft, conversion, negligence, or battery – the identity of the primary wrongdoer is readily

---

[39] 17 U.S.C. §§ 512(a), 512(c). See discussion in Part II.C, *infra*.
[40] Communications Decency Act of 1996, § 230. See discussion in Part II.C, *infra.*
[41] See *supra* note 2.

apparent, and it is usually not an intermediary. Even if a third party facilitates the wrong, the actual wrongdoer is generally easy enough to distinguish from that third party. If I steal from you and deposit the proceeds into my bank account, the bank may be secondarily liable for some aspects of my conduct[42] and may be subject to a garnishment order in relation to the stolen funds.[43] However, it is clear that the bank – the intermediary – is not the primary wrongdoer. I am.

Online, however, it is often difficult to discern who is most appropriately identified as the *primary* wrongdoer. In *Playboy Enterprises v Netscape*, for example, it was unclear to the Ninth Circuit Court of Appeals whether the Netscape search engine should be regarded as a primary or secondary infringer of Playboy's trademarks.[44] Netscape's advertising system allowed its paying advertisers to link their advertisements to terms pre-identified by Netscape as common search terms in the advertiser's field. Thus, a dog food company might pay to have its advertisements keyed to search results when an Internet user enters a search query related to dogs.[45]

Playboy complained that Netscape included Playboy's trademarked terms "playboy" and "playmate" for keying advertisements related to adult entertainment.[46] Some of the resulting advertisements were not clearly labeled as to whether they were officially related to Playboy's business.[47] An Internet user clicking on an ad might incorrectly assume he or she was dealing with Playboy or an unaffiliated entity providing similar services. A successful trademark infringement action requires consumers of a product or service to be confused about the source of that product or service.[48]

---

[42] William Blair, *Secondary Liability of Financial Institutions for the Fraud of Third Parties*, 30 HONG KONG L.J. 74 (2000) (noting the basis upon which secondary liability is often imposed on banks and financial institutions in British-based common law systems).

[43] Allen Myers, *Untangling the Safety Net: Protecting Federal Benefits from Freezes, Fees, and Garnishment*, 66 WASH & LEE L. REV. 371, 375-380 (2009) (explaining the basis and nature of a typical garnishment order filed against a bank).

[44] *Playboy Enterprises v Netscape*, 354 F. 3d 1020 (9th Cir. 2004).

[45] *Id.* at 1022-1023 ("Keying allows advertisers to target individuals with certain interests by linking advertisements to pre-identified terms. To take an innocuous example, a person who searches for a term related to gardening may be a likely customer for a company selling seeds. Thus, a seed company may pay to have its advertisement displayed when searchers enter terms related to gardening.")

[46] *Id*., at 1022-1023 (describing the nature of the plaintiff's claim).

[47] *Id*., at 1023 ("[Plaintiff] introduced evidence that the adult-oriented banner ads displayed on defendants' search results pages are often graphic in nature and are confusingly labeled or not labeled at all.")

[48] *Id.,* at 1024 ("The 'core element of trademark infringement,' the likelihood of

Playboy thus claimed infringement with respect to the ambiguously presented advertisements keyed to the terms "playboy" and "playmate".

While ultimately holding Netscape liable for infringement, the Ninth Circuit judges were unsure as to whether Netscape was best described as a *primary* or a *secondary* infringer of Playboy's marks.[49] In many ways, secondary liability for Internet intermediaries makes sense in the most contexts. Intermediaries, by definition, are third parties who facilitate activities between principal actors.

However, online the lines are blurred between primary and secondary actors largely because intermediaries physically control the software code that enables primary actors to engage in wrongful online conduct. The Ninth Circuit court in *Netscape* court did not resolve the issue of primary versus secondary liability, holding that Netscape was liable for infringement on one basis or the other and that there was no need to determine which.[50]

One could convincingly argue either way. It is easy to suggest that the advertisers competing with the plaintiff were primarily liable for infringements because they were the ones who drafted the confusing ads that were then keyed to the plaintiff's trademarks. Alternatively, one could argue that Netscape should be primarily liable because of its choice of the keywords it coded into the system and its broadcasting of the confusing advertisements in search results.

While the characterization of Netscape as a primary or secondary infringer had no practical impact on the decision in this case, in other cases the question of primary versus secondary liability for Internet intermediaries has taken on greater significance. For example, in *Cartoon Network v CSC Holdings*, the Second Circuit Court of Appeals was tasked with ascertaining whether the provider of an interactive digital video recorder (DVR) was primarily or secondarily liable for copyright infringement with respect to content copied to its servers at the request of its customers.[51]

---

confusion, lies at the center of this case.").

[49] *Id.* ("the parties dispute whether a direct or a contributory theory of liability applies to defendants' actions. We conclude that defendants are potentially liable under one theory and that we need not decide which one.")

[50] *Id*. ("Whether the defendants are directly or merely contributorily liable proves to be a tricky question. However, we need not decide that question here. We conclude that defendants are either directly or contributorily liable. Under either theory, [plaintiff's] case may proceed. Thus, we need not decide this issue.")

[51] *Cartoon Network v CSC Holdings*, 536 F. 3d 121 (2008).

Like *Playboy v Netscape*, the facts of this case are unique to cyberspace. They simply could not have arisen in the context of pre-digital video recording technologies. In the good old days of Betamax and VHS tape recorders, it was clear that any primary infringements – unauthorized copies of protected content – were made by *owners* of video recorders.[52] The providers of the copying technology were not involved in the primary infringements because they did not decide which programs were recorded, when, or how often.[53] They did not even know what programs were being recorded by their customers.

These pre-digital intermediaries merely provided the technology that enabled copying. The Supreme Court in 1984 stated as much in the seminal case of *Sony v Universal City Studios,* holding that Sony, as the manufacturer of the Betamax video tape recorder, might be held *secondarily* liable for infringements of copyrighted works carried out by its customers if the customers were primary infringers.[54] The court found no primary infringement on the part of the customers by virtue of the application of the fair use defense.[55]

However, in *Cartoon Network*, the Second Circuit court faced the problem of consumer copying anew in the digital context, the technology enabling copying to now occur remotely over a network. The DVR service in *Cartoon Network* mimicked the functionality of the analog video recorder under consideration in *Sony*, but technically operated quite differently. As with a set-top video recorder, the DVR service provided by the defendant – Cablevision – allowed its customers to record programs from the television. However, unlike analog recorders, Cablevision's service enabled copies to be made remotely and stored on Cablevision's servers.[56] Thus, Cablevision itself physically made the infringing copies of protected television programs at its customers' request and stored on its own servers.[57]

The Second Circuit Court of Appeals held that Cablevision was not a

---

[52] *Sony v University City Studios*, 464 U.S. 417, 446-7 (1984) (characterizing Sony as having no direct involvement with those who copy programs without authorization).

[53] *Id.*

[54] *Id.*

[55] *Id*., at 454-455 (holding that the copying by owners of DVRs was authorized time shifting and thus covered by the fair use defense to copyright infringement)

[56] *Cartoon Network v CSC Holdings*, 536 F. 3d 121, 124-125 (2008) (describing the operation of Cablevision's remote DVR system).

[57] *Id*

direct copyright infringer.[58] According to the court, if there was any infringement, it was the users of the service who effectively made the copies by ordering Cablevision's servers to record them.[59] These users were unlikely to be held liable as direct infringers because of the *Sony* decision. In *Sony*, the Supreme Court had held that television audiences did not infringe copyrights when they recorded programs for later viewing.[60] This practice was labeled "time shifting" and was considered by a majority of the Supreme Court to be a fair use of the copyrighted work.[61] Assuming that Cablevision's customers were largely engaged in time-shifting, the Second Circuit was correct in suggesting that there would be no primary infringement for which Cablevision could be secondarily liable.[62]

While this result seems logical, the Second Circuit had to go to some lengths in its reasoning to avoiding finding Cablevision liable as a direct infringer. Unlike the old Sony Betamax video recorders, Cablevision did in fact make actual copies of protected works at its customers' instigation. Further, unauthorized reproduction of protected works attracts strict liability under the copyright act.[63] The Second Circuit avoided the direct infringement result largely by reading a volition requirement into the copyright act that doesn't literally appear in the statute.[64] Following an

---

[58] *Id*., at 133 ("We conclude only that on the facts of this case, copies produced by the RS-DVR system are 'made' by the RS-DVR customer, and Cablevision's contribution to this reproduction by providing the system does not warrant the imposition of direct liability.")

[59] *Id.*

[60] *Sony v Universal City Studios*, 464 U.S. 417, 456 (1984) ("One may search the Copyright Act in vain for any sign that the elected representatives of the millions of people who watch television every day have made it unlawful to copy a program for later viewing at home, or have enacted a flat prohibition against the sale of machines that make such copying possible.")

[61] *Id*., at 454 ("we must conclude that this record amply supports the District Court's conclusion that home time-shifting is fair use").

[62] *Cartoon Network v CSC Holdings*, 536 F. 3d 121, 130 (2008) ("The question is *who* made this copy. If it is Cablevision, plaintiffs' theory of direct infringement succeeds; if it is the customer, plaintiffs' theory fails because Cablevision would then face, at most, secondary liability, a theory of liability expressly disavowed by plaintiffs.")

[63] JOHN TEHRANIAN, INFRINGEMENT NATION: COPYRIGHT 2.0 AND YOU, 13 (2011) ("copyright law is a strict liability regime with no mens rea requirement for liability").

[64] *Cartoon Network v CSC Holdings*, 536 F. 3d 121, 131 (2008) ("When there is a dispute as to the author of an allegedly infringing instance of reproduction, *Netcom* and its progeny direct our attention to the volitional conduct that causes the copy to be made. There are only two instances of volitional conduct in this case: Cablevision's conduct in designing, housing, and maintaining a system that exists only to produce a copy, and a customer's conduct in ordering that system to produce a copy of a specific program. In the case of a VCR, it seems clear-and we know of no case holding otherwise-that the operator of the VCR, the person who actually presses the button to make the recording, supplies the

earlier Internet intermediary copyright case, the Second Circuit continued to chip away at the strict liability basis of copyright infringement in order to reach the desired result, a result that was consistent with the spirit of the earlier *Sony* case, if not the technical reality.[65]

Questions of primary versus secondary liability for intermediaries come up again and again in different contexts online,[66] and are often resolved inconsistently, partly due to the failure of judges and scholars to focus on synergies between the role of intermediaries across different fields of law. The cyberlaw of the future should focus on the role of the Internet intermediary to enable discussions about primary versus secondary liability to be examined consistently within a cohesive theoretical framework across discrete areas of law. It may be that a general presumption of secondary, rather than primary, liability makes sense for intermediaries because of their nature as 'middlemen' facilitating the conduct of others. However, even within the context of intermediary secondary liability, significant challenges arise.

---

necessary element of volition, not the person who manufactures, maintains, or, if distinct from the operator, owns the machine. We do not believe that an RS-DVR customer is sufficiently distinguishable from a VCR user to impose liability as a direct infringer on a different party for copies that are made automatically upon that customer's command.") See also discussion in Jacqueline Lipton, *Cyberspace, Exceptionalism, and the Role of Intent in Copyright Infringement*, 13 VANDERBILT JOURNAL OF ENTERTAINMENT & TECHNOLOGY LAW 767, 791 (2011) ("The *Cartoon Network* court employed an approach adopted in at least one earlier Internet case involving individual copying that had been enabled by an Internet service provider. The earlier case had imposed a 'volition' requirement in the context of direct infringement. In other words, the plaintiff needed to prove that the defendant's conduct was volitional rather than a largely automated technological process. This volition requirement may be seen as a judicial gloss on strict liability to accommodate technological innovation.") [hereinafter, *Cyberspace Exceptionalism*].

[65] *Cartoon Network v CSC Holdings*, 536 F. 3d 121, 130 (2008), citing *Religious Technology Center v. Netcom On-Line Communications Services,* 907 F. Supp. 1361 (N.D. Cal. 1995).

[66] *Playboy Enterprises v Netscape*, 354 F. 3d 1020 (9th Cir. 2004) (discussion of primary versus secondary liability of search engine in the trademark infringement context); *Cartoon Network v CSC Holdings*, 536 F. 3d 121, 130 (2008) (discussion of primary versus secondary liability of video recording service provider in the copyright infringement context); *Fair Housing Council of San Fernando Valley v Roommate.com*, 521 F. 3d 1157 (9th Cir. 2008) (discussing whether an online housemate matching service could be held primarily liability for content posted by customers that allegedly infringed fair housing legislation).

C. Questions of Secondary Liability

In the early days of the Internet, legal questions about intermediary liability tended to revolve around ISPs that provided bulletin boards and other basic communications forums.[67] Courts were asked whether providers of such forums could be held liable for content posted by their members and, if so, on what basis.[68] The most common claims in the late 1990s related to defamation and copyright.[69]

In the absence of a unified cyberlaw field focusing on ISP liability issues in the 1990s, courts and legislators took a silo-ed approach to questions of ISP liability, considering each situation largely within the context of the distinct legal wrong involved. Thus, lawmakers may have missed significant critical points in the development of Internet law to ensure a systematic consideration of principles of Internet intermediary liability. The law on ISP liability for defamation and copyright evolved, first through common law, and later through legislation, in a piecemeal fashion. Today it is difficult to reconcile the principles of ISP liability for defamation with those of ISP liability for copyright infringement.

In early defamation cases, for example, courts generally exempted ISPs from liability for defamatory comments posted by others provided that the ISP had not itself exercised significant editorial control over the content.[70] This soon proved problematic because it effectively penalized ISPs that were attempting to "do the right thing" and censor inappropriate conduct.

---

[67] *Cubby v Compuserve*, 776 F. Supp. 135 (S.D.N.Y. 1991) (considering liability of ISP for allegedly defamatory content posted by its customers); *Stratton Oakmont v Prodigy*, 1995 WL 323710 (N.Y. Sup. May 24, 1995) (considering liability of ISP for allegedly defamatory comments posted by customers); *Playboy Enterprises v Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993) (considering liability of bulletin board operator for copyright infringements of those posting on the bulletin board); *Religious Technology Center v Netcom*, 907 F. Supp. 1361 (N.D. Cal. 1995) (considering extent to which ISP and operator of bulletin board service could be held liable for copyright infringements of those posting information on the bulletin board)

[68] *Cubby v Compuserve*, 776 F. Supp. 135 (S.D.N.Y. 1991) (considering liability of ISP for allegedly defamatory content posted by its customers); *Stratton Oakmont v Prodigy*, 1995 WL 323710 (N.Y. Sup. May 24, 1995) (considering liability of ISP for allegedly defamatory comments posted by customers).

[69] See *supra*, note 67.

[70] *Cubby v Compuserve*, 776 F. Supp. 135 (S.D.N.Y. 1991) (ISP not liable for defamatory content posted by others); *Stratton Oakmont v Prodigy*, 1995 WL 323710 (N.Y. Sup. May 24, 1995) (ISP was liable for comments posted by others because it was said to have exercised significant control over content through its family friendly monitoring practices).

The more active the ISP was in, say, protecting children from harmful material, the more likely it would be to attract legal liability.[71] ISPs that turned a blind eye to the content of communications were more likely to escape legal liability than those that were pro-active about monitoring content.[72]

Congress eventually intervened, enacting § 230 of the Communications Decency Act (CDA). This section, in relevant part, provides that: "No provider … of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[73] Courts interpreted this provision as almost a blanket immunity for ISPs with respect to defamatory comments posted by others.[74] In one case, an ISP was exempted from liability even though it had contracted with a columnist to contribute provocative content that it knew was likely to be defamatory.[75] In another case, an ISP was held to be immune where it had been made aware of damaging false comments and had failed to remove them in a timely fashion.[76] To date, ISPs have only been held liable as information content providers under § 230 where they have actually *written* the relevant content themselves.[77]

The current position on ISP liability for defamation differs dramatically from the position on ISP liability for copyright infringement. Initially, when Internet users posted copyrighted content on bulletin boards, courts struggled to determine whether the ISPs that provided the forums should be

---

[71] *Stratton Oakmont v Prodigy*, 1995 WL 323710 (N.Y. Sup. May 24, 1995) (holding family friendly ISP liable for allegedly defamatory comments posted by customers because of its attempts to monitor content, suggesting it should have controlled content more effectively).

[72] *Id*., at 13 ("PRODIGY's conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability than CompuServe and other computer networks that make no such choice.")

[73] 47 U.S.C. § 230(c)(1).

[74] David Lukmire, *Can the Courts Take the Communications Decency Act? The Reverberations of Zeran v America Online*, 66 N.Y.U. ANN. SURV. AM. L. 371, 372 (2010) ("Over the years, state and federal courts have interpreted section 230 expansively, conferring a broad immunity upon website operators that host third-party content. The statute has grown into a 'judicial oak,' with impacts far beyond its language sounding in defamation law and its original intent to prevent the nascent Internet from becoming a 'red light district.'")

[75] *Blumenthal v Drudge*, 992 F. Supp. 44 (D.D.C. 1998).

[76] *Zeran v America Online*, 129 F. 3d 327 (4th Cir. 1997).

[77] *Fair Housing Council of San Fernando Valley v Roommate.com*, 521 F. 3d 1157 (9th Cir. 2008) (but note that this was not a defamation case, but rather a case involving alleged infringements of fair housing legislation).

held liable for those infringements.[78] Ultimately, Congress stepped in to ensure that ISPs were not held liable for copyright infringement when they were acting as mere conduits or repositories for the postings of others.[79]

Congress enacted the Online Copyright Infringement Liability Limitation Act (OCILLA) as part of the Digital Millennium Copyright Act (DMCA) package of 1998. OCILLA provides a safe harbor for ISPs in the case of non-volitional or non-willful copying: in other words, copying that occurs as part of a purely technical or mechanical process and that was initiated by another person.[80] The statute also exempts ISPs from liability where the ISP had no actual or constructive knowledge of the infringement, had not directly benefited from the infringement, and had responded expeditiously to a request to remove infringing content.[81]

The ISP safe harbors for defamation and copyright were enacted around the same time.[82] However, the respective statutes clearly follow different approaches. This result is not surprising given that the drafters of OCILLA were focused on amending the copyright act for the digital age, while the drafters of the CDA were dealing with a broader statute about protecting children from harmful material online.[83] Both statutes would have been incredibly challenging to draft,[84] particularly in the early days of the Internet when it was unclear how relevant technologies would develop and how people would use them, and indeed what role Internet intermediaries would ultimately play in monitoring online communications.

Nonetheless, there were significant commonalities in aim between the statutes, at least in the case of the ISP safe harbor provisions. Drafters of both statutes were faced with the emerging role of the Internet intermediary

---

[78] *Playboy Enterprises v Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993) (considering ISP liability for copyright infringement); *Religious Technology Center v Netcom*, 907 F. Supp. 1361 (N.D. Cal. 1995) (considering copyright infringement liability of ISP and bulletin board operator).

[79] 17 U.S.C. § 512.

[80] 17 U.S.C. § 512(a).

[81] 17 U.S.C. § 512(c). The statute also exempted ISPs from liability for system caching ie temporary housing of copies of digital information: 15 U.S.C. § 512(b).

[82] Section 230 of the CDA was enacted in 1996 while OCILLA was enacted in 1998.

[83] Lukmire, *supra* note 74, at 373-378 (describing the legislative history of the Communications Decency Act as being an attempt to constitutionally incentivize website operators to police the Internet and to prevent minors from accessing harmful content).

[84] In fact, significant portions of the CDA (other than § 230) failed to pass constitutional muster in the face of First Amendment challenges. See *Reno v A.C.L.U.*, 521 U.S. 844 (1997) (striking down other sections of the legislation for creating impermissibly overbroad constraints on online communication).

and questions about the impact of imposing liability upon intermediaries for wrongs committed by others. However, each drafting group understandably focused on its own brief without examining the nature of ISP liability more generally.

In the final analysis, it is possible to reconcile the approaches taken by Congress respectively in OCILLA and in § 230 of the CDA, although the reconciliation may be somewhat unsatisfying as an *ex post facto* rationalization. For example, one might argue that it is easier for an ISP to have knowledge of a copyright infringement than of the veracity of a defamation claim because copyrights are generally registered[85] and because OCILLA requires the claimant to give detailed notice to the ISP of a copyright claim.[86] Thus, it is arguably reasonable to hold ISPs liable for copyright infringement on the basis of notice but to exempt them from defamation liability regardless of notice. It is at least theoretically much easier for an ISP to make a reasonable judgment about the veracity of a copyright claim than about the legitimacy of a defamation claim.

Of course, one could argue that if an ISP is not in a good position to make decisions about the merits of a defamation claim, then the ISP should err on the side of protecting the claimant's reputation and should be exposed to liability if it fails to act. However, this opens intermediaries up to potentially frivolous claims that cannot be easily verified. If an intermediary is required to act on each claim by removing offending material – or at least investigating the merits - the resulting costs to those service providers may be prohibitive. There is no easy way for an ISP to determine whether posted comments are defamatory or not, as opposed to a copyright claim where registration of a copyright is at least prima facie evidence of its validity.[87]

In all contexts, Internet intermediaries are routinely put in the unenviable position of either erring on the side of facilitating the free flow of ideas online or of monitoring and policing content. Where the content involves potentially infringing rights the existence of which can be relatively easily verified by the intermediary, it might be reasonable to impose liability on the intermediary if it fails to act. In other circumstances,

---

[85] TEHRANIAN, *supra* note 63, at 98 (noting the necessity of registering copyrighted works in the United States in order to obtain meaningful judicial relief for infringement).

[86] 17 U.S.C. §(c)(3)(A).

[87] MARHSALL LEAFFER, UNDERSTANDING COPYRIGHT LAW, 273(5 ed, 2010) (noting that registration of a copyright "confers prima facie evidence of the validity of the copyright").

liability might be less appropriate absent a showing of complicity by the intermediary in the wrongful conduct.

One might criticize the different approaches taken between OCILLA and § 230 of the CDA. In fact, it is interesting that there is so little commentary on the comparison between the two approaches in current literature. In both defamation and copyright claims, ISPs have been put into the position of making difficult decisions about whether or not to act in the face of a complaint. In both cases they have had to examine the extent to which they might be regarded as complicit in the alleged wrong. And in both cases they have been put in the position of making decisions that impact on free expression: that is, to remove content and risk being criticized for censorship or to allow allegedly infringing content and risk being sued as complicit in the commission of an online wrong. However, Congress acted in a way that misses these synergies, taking one approach with respect to copyrights and another with respect to defamation and other harmful content.

D. Benefits of a Renewed Focus on Intermediary Liability

Refocusing the cyberlaw field as a law of the intermediated information exchange would create an effective theoretical framework within which to investigate the commonalities between facially disparate areas of law like intermediary liability for defamation and copyright infringement. There is a pressing need to develop such a theoretical framework. New issues of intermediary liability are constantly arising, often requiring novel applications of existing legal principles.[88]

The lack of a coherent theoretical framework governing the liability of Internet intermediaries for online wrongs is exemplified in debates over SOPA.[89] This bill grants power to the Attorney General to bring actions against owners of websites that host content that infringes American intellectual property rights.[90] It also imposes significant obligations on online service providers to comply with court orders made under the legislation.[91] These obligations include increased policing and monitoring

---

[88] LOWE, *supra* note 32, at 213 ("From patent, copyright, and trademark infringement to click fraud to wrongful dismissal, Google spends a lot of time in court. While it is true that Google makes a large target, it also is true … that it is operating in a field littered with uncertainties begging to be resolved in the courts of law. Some of the lawsuits address key issues that could define both Google and the Internet of the future.")

[89] See *supra* note 1.

[90] H.R. 3261 1H (112th Cong.), §102(b).

[91] *Id.*, §102(c).

of content being transmitted via their services.[92] The new legal duties, if implemented, would place new burdens on service providers including search engines,[93] online payments systems,[94] and online advertising services.[95]

While this legislation is aimed at the protection of intellectual property rights in particular, it covers the same issues that arise in relation to the enforcement of other laws in cyberspace. It deals with finding an appropriate framework for imposing legal obligations on online service providers with respect to wrongs committed by others. The drafters of the bill, like those of the legislation described in the previous sub-Part, are faced with the competing aims of encouraging online innovation and preventing online harm. Additionally, as with the CDA and OCILLA, the drafters of SOPA have latched on to the reality that online service providers can be the most effective choke points in online interaction to interrupt the flow of infringing or harmful communications.

Lobbyists for free speech and privacy argue that SOPA strikes the balance too heavily in favor of protecting proprietary content and will negatively impact the online marketplace of information and ideas.[96] Those representing the digital content industries take the view that legislation aimed at blocking the online flow of infringing content is necessary to protect innovation in digital content production and distribution.[97] As with the CDA and OCILLA, the online intermediaries effectively become the meat in the sandwich between those who advocate free speech and privacy, and those who seek to prevent intellectual property infringement. A more comprehensive and cohesive theoretical framework within which to consider the appropriate role for online service providers in these contexts would be extremely helpful in furthering more balanced drafting of legislation such as SOPA.

Of course, SOPA has been drafted in its current form in the context of existing caselaw dealing with the role of online intermediaries for the intellectual property infringements of others. This caselaw may not have given Congress particularly effective guidance in drafting legislation aimed

---

[92] *Id.*

[93] *Id.,* §102(c)(2)(B).

[94] *Id.,* §102(c)(2)(C).

[95] *Id.,* §102(c)(2)(D).

[96] Goodman, *supra* note 1 ("Information is the currency of democracy, and people will not sit still as moneyed interests try to deny them access.")

[97] *Id*. (describing the aims of the legislation from the point of view of copyright holders).

at balancing online information flow against the need to prevent widespread copyright infringement. Two relatively recent Ninth Circuit decisions handed down prior to the drafting of SOPA went in two different directions on the potential copyright infringement liability of an Internet search engine and a group of electronic payments system providers respectively.

The respective defendants were the Google search engine in one case, and the Visa online payments system in the other.[98] The plaintiff in each case was Perfect 10, a company whose business was selling photos of nude models online.[99] In the litigation against Google, Perfect 10 claimed copyright infringement in respect of unauthorized reproductions and displays of its copyrighted photographs that showed up in Google's search results.[100] Perfect 10 claimed both direct and indirect infringement, arguing that Google should be held responsible for its own reproductions and displays of the copyrighted photographs in its search engine results.[101] It should also be held secondarily liable for the infringements by the people who had actually made the illegal copies in the first place where the copies showed up in search results.[102] In the litigation against Visa, Perfect 10 claimed only secondary liability with respect to Visa enabling payments to companies that sold unauthorized reproductions of Perfect 10's protected photographs.[103]

---

[98] *Perfect 10 v Google*, 508 F. 3d 1146 (9th Cir. 2007); *Perfect 10 v Visa*, 494 F. 3d 788 (9th Cir. 2007).

[99] *Perfect 10 v Google*, 508 F. 3d 1146, 1157 (9th Cir. 2007) ("Perfect 10 markets and sells copyrighted images of nude models. Among other enterprises, it operates a subscription website on the Internet. Subscribers pay a monthly fee to view Perfect 10 images in a 'members' area' of the site.")

[100] *Id.*, at 1159 ("Perfect 10 claims that Google's search engine program directly infringes two exclusive rights granted to copyright holders: its display rights and its distribution rights").

[101] *Id.*, at 1163 (noting that plaintiff had succeeded in establishing a prima facie case that Google had infringed its copyrights by reproducing copyrighted photographs as thumbnail images); but see 1168 (court ultimately held that Google's reproductions of the images as thumbnails in its search engine results page was a fair use and therefore non-inringing).

[102] *Id.*, at 1170 (describing the need to evaluate: "Perfect 10's arguments that Google is secondarily liable in light of the direct infringement that is undisputed by the parties: third-party websites' reproducing, displaying, and distributing unauthorized copies of Perfect 10's images on the Internet").

[103] *Perfect 10 v Visa*, 494 F. 3d 788, 792 (9th Cir. 2007) ("Perfect 10, Inc. (Perfect 10) sued Visa International Service Association, MasterCard International Inc., and several affiliated banks and data processing services (collectively, the Defendants), alleging secondary liability under federal copyright … law …. It sued because Defendants continue to process credit card payments to websites that infringe Perfect 10's intellectual property rights after being notified by Perfect 10 of infringement by those websites.")

With respect to the secondary liability claims, the court ultimately held that Google could potentially be contributorily liable for the copyright infringements, but that there were factual matters to be reconsidered on remand.[104] However, with respect to Visa, the court held no secondary liability on the basis that Visa's activities were too far removed from the primary infringements to be regarded as contributing to those infringements.[105] In distinguishing the *Google* case, the court noted in *Visa* that: "The salient distinction is that Google's search engine itself assists in the distribution of infringing content to Internet users, while [Visa's] payments systems do not."[106] The majority in Visa admitted that Visa assists in making the primary infringements *profitable*, but they distinguished the profitability of the infringement from the distribution and availability of infringing images online.[107]

The *Visa* case included a strong dissent from Judge Kozinski who argued that the payments system provides more than a mere economic incentive to infringe, but actually provides "an essential step in the infringement process".[108] In Judge Kozinski's view, without the payments

---

[104] *Perfect 10 v Google*, 508 F. 3d 1146, 1172-1173 (9th Cir. 2007) ("Google could be held contributorily liable if it had knowledge that infringing Perfect 10 images were available using its search engine, could take simple measures to prevent further damage to Perfect 10's copyrighted works, and failed to take such steps. The district court did not resolve the factual disputes over the adequacy of Perfect 10's notices to Google and Google's responses to those notices. Moreover, there are factual disputes over whether there are reasonable and feasible means for Google to refrain from providing access to infringing images. Therefore, we must remand this claim to the district court for further consideration whether Perfect 10 would likely succeed in establishing that Google was contributorily liable …")

[105] *Perfect 10 v Visa*, 494 F. 3d 788, 796 (9th Cir. 2007) ("The credit card companies cannot be said to materially contribute to the infringement in this case because they have no direct connection to that infringement. Here, the infringement rests on the reproduction, alteration, display and distribution of Perfect 10's images over the Internet. Perfect 10 has not alleged that any infringing material passes over Defendants' payment networks or through their payment processing systems, or that Defendants' systems are used to alter or display the infringing images. … While Perfect 10 has alleged that Defendants make it easier for websites to profit from this infringing activity, the issue here is reproduction, alteration, display and distribution, which can occur without payment.")

[106] *Id.*, at 797.

[107] *Id*. ("[Visa] do[es], as alleged, make infringement more profitable, and people are generally more inclined to engage in an activity when it is financially profitable. However, there is an additional step in the causal chain: Google may materially contribute to infringement by making it fast and easy for third parties to locate and distribute infringing material, whereas [Visa] make[s] it easier for infringement to be *profitable*, which tends to increase financial incentives to infringe, which in turn tends to increase infringement.")

[108] *Id*., at 812.

systems, infringement would be almost impossible.[109] Clearly, there is room for disagreement as to where to draw the secondary liability line when it comes to Internet gatekeepers. An appropriately reconceptualized cyberlaw field would provide a much needed theoretical framework within which to reconsider these issues.

While providing accessible and innovative services to enable individuals to interact more efficiently and effectively, online service providers are subject to the possibility of secondary liability claims for activities about which they have little actual knowledge: including copyright, defamation, trademark infringement, bullying, harassment liability etc. Courts are likely to be faced with questions about what an intermediary *could* or *should* have known about the activities of a primary infringer in a number of these different contexts. These questions are not unique to copyright law.

As intermediaries' business operations continue to scale up, they may be less and less sure of what all their users are doing. In remanding the *Google* case back to the lower court, the Ninth Circuit was mindful that it had insufficient information about the realities of Google's position to make a meaningful determination on contributory liability for copyright infringement. All it held was that liability was *possible* on this basis, but it wanted the lower court to look more closely at the position Google was actually in, and whether Google realistically had the capabilities to detect and prevent copyright infringement.[110]

Courts and legislatures will continue to face questions of the secondary liability of online intermediaries in copyright and other areas of law. However, to date these issues have been tackled on a subject matter basis. SOPA and OCILLA are both confined to the position of Internet intermediaries with respect to copyright infringements. Section 230 of the

---

[109] *Id.*("My colleagues recognize, as they must, that helping consumers locate infringing content can constitute contributory infringement, but they consign the means of payment to secondary status…. But why is *locating* infringing images more central to infringement than *paying* for them? If infringing images can't be found, there can be no infringement; but if infringing images can't be paid for, there can be no infringement either…")

[110] *Perfect 10 v Google*, 508 F. 3d 1146, 1172-1173 (9th Cir. 2007) ("there are factual disputes over whether there are reasonable and feasible means for Google to refrain from providing access to infringing images. Therefore, we must remand this claim to the district court for further consideration whether Perfect 10 would likely succeed in establishing that Google was contributorily liable for in-line linking to full-size infringing images under the test enunciated today.")

CDA, on the other hand, considers similar issues with respect to other online conduct such as defamation and other forms of harmful speech outside the intellectual property arena.[111]

Current cyberlaw scholars tend to consider each specific question within a vacuum or silo without looking at the role of Internet intermediaries more broadly. As cyberlaw is in reality the law of intermediated information exchange, a debate that is refocused more specifically on the role of online intermediaries has a better chance of achieving consistency of application than the current piecemeal approach.

E. Responsibilities to Unmask Online Wrongdoers

Another advantage of refocusing cyberlaw on the role of Internet intermediaries would be that such a move would provide a theoretical paradigm within which to consider the unique role of intermediaries in terms of their potential to *unmask* online wrongdoers. Internet intermediaries are often in the position of being the only entity within a given dispute capable of identifying or locating an online wrongdoer even in circumstances where the intermediary itself is not complicit in committing the harm. Much online communication is anonymous or pseudonymous.[112] Thus, victims of online wrongs cannot identify the person or persons engaging in harmful conduct.

However, again, the law must strike a delicate balance between ensuring that intermediaries assist in unmasking wrongdoers while at the same time avoiding a chilling effect on intermediaries' business models. If intermediaries are too often and too easily required to identify customers who wish to remain anonymous, this will likely result in a chilling of online activity. This has been one of the most marked criticisms of SOPA – involving the extent to which the legislation would require online service providers to take responsibility for policing online wrongdoers and potentially infringing the privacy and autonomy of their customers in the process.[113]

---

[111] 47 U.S.C. § 230(e)(2)(" Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.")

[112] Lipton, *supra* note 37, at 1114 ("The anonymity provided by the Internet may increase the volume of abusive conduct because it may encourage individuals who would not engage in such conduct offline to do so in the anonymous virtual forum provided by the Internet.")

[113] H.R. 3261 1H (112th Cong.), § 102(c).

There is a delicate balance to be struck between the obligations of Internet intermediaries to law enforcement and to their customer bases.[114] Internet users may be loathe to communicate online for fear of being unmasked if there is excessive obligation on intermediaries to police their activities.[115] Intermediaries may also falter in the marketplace if they cannot protect their customers' privacy sufficiently.[116] The requirement that intermediaries stand ready to unmask their customers also imposes costs on intermediaries related to obtaining and maintaining sufficiently detailed records to identify customers when necessary.

To date, courts have developed rules to determine the circumstances under which an Internet intermediary may be ordered to divulge the identity of an alleged defendant[117] or a witness to an online wrong.[118] In these cases, judges have had to draw lines that most appropriately balance the interests of an intermediary in protecting its members' anonymity against the interests of a complainant. Judges have faced these challenges in the context of cases involving copyright infringement,[119] defamation,[120] trademark infringement,[121] and complaints about reputational harm.[122]

A broader look at these questions through the lens of Internet

---

[114] And increasingly as online service providers such as Facebook become public corporations, they will be faced with additional obligations to shareholders.

[115] Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace*, 104 YALE L. J. 1639, 1641 (1995) (noting the trend for Internet users to desire to speak without censorship and to take advantage of the Internet's relative anonymity in doing so)

[116] *Id*., at 1671 ("The Networld has an abundance of opportunities for full and uninhibited speech. The difficulty has become one of offended parties seeking to inhibit the speech of the offending posters of messages. As the offended turn to their lawyers to redress their grievances, this uninhibited cauldron of opinion becomes threatened. Should strict liability for all electronic transmission become the accepted norm, service providers might scramble to hide behind contracts, waivers, monitoring of all content, and censorship of messages before posting …. Liability insurance would be prohibitively expensive, the burden of monitoring all messages before posting them too demanding, and the possibility of facing protracted litigation too onerous.")

[117] *Columbia Ins. Co. v SeesCandy.Com*, 18 F.R.D. 573 (N.D. Cal. 1999); *In re Subpoena Duces Tecum to America Online*, 52 Va. Cir. 26 (2000); *Doe I and Doe II v Individuals, Whose True Names Are Unknown*, Civil Action No. 3:07 CV 909 (CFD), 2008 WL 2428206 (D. Conn. June 13, 2008).

[118] *Doe v 2TheMart.Com*., 140 F. Supp. 2d 1088 (W.D. Wa. 2001).

[119] *In re Verizon Internet Services*., 257 F. Supp. 2d 244 (D.D.C. 2003).

[120] *In re Subpoena Duces Tecum to America Online*, 52 Va. Cir. 26 (2000).

[121] *Columbia Ins. Co. v SeesCandy.Com*, 18 F.R.D. 573 (N.D. Cal. 1999).

[122] *Doe I and Doe II v Individuals, Whose True Names Are Unknown*, Civil Action No. 3:07 CV 909 (CFD), 2008 WL 2428206 (D. Conn. June 13, 2008).

intermediary liability more generally would enable more cohesive and systematic rules to develop over time. The development of clearer rules about the responsibility of intermediaries to maintain and divulge identifying records about customers would assist in making business more predictable for intermediaries and their customers. This predictability may also be useful to victims of online wrongs as they would gain a better *ex ante* sense of the likelihood of unmasking a potential defendant or witness in a given situation.

The role of the Internet intermediary is effectively the foundation of cyberlaw, or at least it should be. Intermediaries are necessary for all online interaction. No one can communicate online without using at least one intermediary. Intermediaries are the gatekeepers to all we do online. They hold great power in the sense of enabling access to online communications, setting the parameters of online conduct through their software coding, and maintaining records of the identities of online actors. They can also be the most effective choke points to prevent harmful online interactions.

However, imposing legal responsibilities on intermediaries always comes at a cost. The more duties legally imposed on intermediaries, the more likely the result will be a chilling of online innovation. Reconceptualizing cyberlaw as a field the primary focus of which is to address these issues would lead to significant benefits in terms of creating greater certainty for online service providers and their customers with respect to their legal rights and obligations.

III. JURISDICTION

Any reconceptualization of the cyberlaw field should retain some focus on major jurisdictional challenges created by cyberspace interactions. Again, Internet intermediaries will often be key players in jurisdictional disputes as they are the parties that enable the global communications and they are often the easiest parties for a defendant to locate. Additionally, a court order against an intermediary will likely be more effective than an order against often multiple individual defendants because the intermediaries are the choke points for communications. If an intermediary is ordered to remove or monitor the flow of certain information, the result will be more effective than an order against a private defendant who may use aliases or pseudonyms, as well as effectively being able to mask his or

her location, and being judgment proof.[123]

When global communications were easily, quickly, and cheaply enabled in the 1990s by the widespread public take-up of the Internet, it seemed obvious that the major new legal issues would be jurisdictional. The Internet opened up seemingly endless possibilities for litigating against foreign defendants, raising choice of law and choice of forum questions as well as foreign enforcement challenges.[124] Even if a court in the plaintiff's jurisdiction agreed to exercise jurisdiction over a foreign defendant and an order was obtained in favor of the plaintiff, it would not always be clear that the order could be enforced in the foreign jurisdiction. Particularly problematic have been cases where the defendant holds no assets in the plaintiff's jurisdiction that might be attached as part of a judgment order. The ongoing litigation between Yahoo! and La Ligue contre le Racisme et l'Antisemitisme in France is a good example highlighting uncertainties about how, or indeed if, a court order from the plaintiff's country might be enforced in the defendant's country.[125]

In the *Yahoo!* litigation, a French plaintiff successfully obtained a French court order to have Yahoo! enjoined from facilitating sales of Nazi memorabilia in France.[126] Subsequently, Yahoo! took up the matter in California and attempted to obtain a declaration from the Californian courts that the French order could not be enforced against Yahoo!'s assets in California.[127] To date, the Californian courts have refrained from giving a definitive answer to this question.[128] The Californian courts have been split on whether the case is ripe for a decision, and as to whether the Californian courts can exercise personal jurisdiction over the French organization.[129] The United States Supreme Court has denied certiorari,[130] so ultimately any

---

[123] See *supra* note 37.

[124] See, for example, discussion in Michael Gilden, *Jurisdiction and the Internet: The "Real World" Meets Cyberspace*, 7 ILSA J INT'L & COMP L 149 (2000).

[125] *Ligue Contre Le Racisme et L'Antisemitisme v Yahoo!*, Superior Court of Paris (Nov. 20, 2000).

[126] *Id.*

[127] *Yahoo! v La Ligue Contre le Racisme et L'Antisemitisme*, 433 F.3d 1199 (2006).

[128] *Id*., at 1224 ("An eight-judge majority of the en banc panel holds… that the district court properly exercised specific personal jurisdiction over defendants LICRA and UEJF …. A three-judge plurality of the panel concludes … that the suit is unripe for decision ….. When the votes of the three judges who conclude that the suit is unripe are combined with the votes of the three dissenting judges who conclude that there is no personal jurisdiction over LICRA and UEJF, there are six votes to dismiss Yahoo!'s suit.")

[129] *Id.*

[130] *La Ligue Contre le Racisme et l'Antisemitisme v. Yahoo!.*, 547 U.S. 1163 (2006) (denying cert.).

decision made will be in a lower court in California.

Jurisdictional questions are of course not new to cyberspace. However, the Internet raises new challenges for conflicts of law by its very nature. When addressing jurisdictional issues in cyberspace, courts have often complicated their analyses by focusing on the hardware aspects of the Internet. For example, at a loss for guidance on how to ascertain whether a defendant could be said to have purposefully availed herself of the plaintiff's forum,[131] early cyberspace cases tended to focus on the location of physical computer servers.[132] This approach led to random and unpredictable results because of the nature of the Internet.[133] The whole point of the network is that electrons flow relatively randomly through cables (and now wirelessly) to avoid a single point of failure bringing down the entire network.[134] Thus, premising jurisdictional queries on electron flows is unlikely to lead to principled or predictable legal rules.

One reason for the tendency to focus on the physical aspects of the network derived from difficulties inherent in the other obvious option – to consider where the defendant actually engaged in the harmful conduct. When the defendant's conduct is an online communication, and that communication is accessible globally, the purposeful availment inquiry is not very meaningful.[135] If a defendant posts, say, a defamatory comment about a plaintiff on a blog that is accessible globally, is it fair to say that the defendant has purposely availed herself of the jurisdiction of the entire world?[136]

---

[131] Purposeful availment is a prong of a specific personal jurisdiction inquiry and focuses on the defendant's activities within the plaintiff's forum. See, for example, discussion of the concept in *Yahoo! v La Ligue Contre le Racisme et L'Antisemitisme*, 433 F.3d 1199, 1205-1207 (2006).

[132] See, for example, *Bochan v La Fontaine*, 68 F. Supp. 2d 692 (E.D. Va. 1999) (personal jurisdiction hinged on fortuitous location of servers accessed by defendants).

[133] Raymond Shih Ray Ku, *Open Internet Access and Freedom of Speech: A First Amendment Catch-22*, 75 TUL. L. REV. 87, n 38 (2000) ("The TCP/IP protocols break down information transmitted on to the Internet into packets and reassemble it at its destination …. This allows the Internet to operate as a packet-switched network where the various data packets may travel different routes to reach the same destination ….. This design allows information to be transmitted through the Internet at faster speeds than circuit-switched networks, where, once a connection is made, that part of the network is dedicated only to that connection.")

[134] *Id.*

[135] See *supra* note 131.

[136] *Dow Jones v Gutnick*, [2002] HCA 56 (10 Dec. 2002), at para. 54 (noting defamation defendant's concern about being haled into court in any jurisdiction in which its online publications were accessed).

Another alternative is to create a blanket rule that the appropriate jurisdiction for litigation is the place where the plaintiff suffers harm. Several courts have taken this approach,[137] and it certainly seems logical at least from the plaintiff's point of view. One could easily argue that plaintiffs in, say, defamation suits should not have to go to foreign courts to sue defendants who may be taking advantage of their geographical distance, or from more lenient defamation laws in a particular jurisdiction.

However, erring on the side of the plaintiff's jurisdiction may not be particularly fair to the online defendant. If a defendant is potentially to be held liable for any comments made online under the laws of any jurisdiction in which a plaintiff resides or does business, it may be impossible for that defendant to protect itself from unexpected foreign litigation. The reality is that many defendants today do not even know where a plaintiff is located or where she might suffer harm.

The fact that defendants could face significant risks of litigation in foreign jurisdictions under a rule that favored the plaintiff's jurisdiction may ultimately chill much online speech. Defamation defendants have argued against such a rule in past litigation.[138] These concerns come into sharp relief in situations where defendants are increasingly amateur journalists and social commentators, rather than large scale media conglomerates, as is increasingly the case online.[139] Small individual defendants are less likely than a large media outlet to possess the wherewithal to defend proceedings in a foreign jurisdiction.

While there are a number of counter-arguments to concerns about unfairness to defendants,[140] the point of this discussion is not to identify the

---

[137] *Id*., at para. 44 ("ordinarily, defamation is to be located at the place where the damage to reputation occurs. Ordinarily that will be where the material which is alleged to be defamatory is available in comprehensible form assuming, of course, that the person defamed has in that place a reputation which is thereby damaged."); *Calder v Jones*, 465 U.S. 783 (1984) (granting jurisdiction over an out-of-state defendant with respect to a defamation action that harmed the plaintiff – actress Shirley Jones – in California).

[138] *Gutnick v Dow Jones,* VSC 305, para. 56 (Aug. 28, 2001) (*aff'd*, *Dow Jones v Gutnick*, [2002] HCA 56 (10 Dec. 2002)) (noting American publishers significant concerns at being haled into court in Australia for an article it published allegedly defaming an Australian resident).

[139] The observation that journalism is become more of an amateur sport in the Internet age is made forcible in: ANDREW KEEN, THE CULT OF THE AMATEUR (2007).

[140] *Dow Jones v Gutnick*, [2002] HCA 56, para. 53 (10 Dec. 2002) (arguing that damages award will only be made in a defamation case where the plaintiff realistically has a reputation to harm in the place where publication is received); para. 56 (noting that

correct rule on personal jurisdiction in cyberspace. Rather, it is to demonstrate that cyberspace raises unique challenges in terms of jurisdiction. It is necessary within the cyberlaw field to investigate factors that differentiate cyberspace from physical space in the context of these jurisdictional challenges.

Unlike physical world publications, information disseminated over the Internet can generally be received anywhere in the world, subject only to technological limitations such as firewalls and encryption. Thus the default position in Internet publication is effectively opposite to that in the physical world. Online information defaults to being published to everyone globally whereas in the physical world, information is only published to those to whom the publisher has specifically directed it. Thus, the risk of being haled into court in an unexpected foreign jurisdiction is significantly higher for a defendant in an Internet case than in a physical world case. SOPA itself recognizes the problem inherent in global online communications through its attempt to impose monitoring obligations on domestic ISPs to limit infringing activities conducted or facilitated by foreign actors.[141]

The Internet may raise additional challenges related to jurisdiction. In Internet-based litigation, there is a high risk that the initial focus of the litigation will be on jurisdictional issues, rather than on the substance of the plaintiff's complaint. Because of the disproportionately high number of jurisdictional issues in cyberspace cases in comparison with physical world cases, a greater number of cyberspace cases might be disposed of at the jurisdictional stage without ever getting to a determination of the parties' substantive rights. The cyberlaw field can provide a forum within which jurisdictional rules may be streamlined and harmonized. Such a result would then minimize the time and expense necessary on initial jurisdictional questions, and would allow judges to focus more on exploring and developing the substantive rights and obligations of parties in cyberspace disputes.

A recent example of a case in which jurisdictional considerations arguably detracted from an investigation of the plaintiff's substantive rights

---

plaintiffs are unlikely to sue in a jurisdiction outside the defendant's forum unless a judgment in that forum would be of real value to the plaintiff and the answer to that question may depend on whether, and to what extent, the defendant holds assets in the plaintiff's forum); para 56 (noting that in "all except the most unusual of cases, identifying the person about whom material is to be published will readily identify the defamation law to which that person may resort").

[141] H.R. 3261, 1H (112th Cong.), § 102(a).

is *Chang v Virgin Mobile*.[142] In this case, Chang brought *inter alia* a privacy claim against Virgin Mobile for unauthorized use of a photograph of her in an advertising campaign.[143] Chang resided in Texas while the advertising campaign took place in Australia. Virgin Mobile had found the picture of Chang online and copied it from a public photo-sharing website. Virgin Mobile had only utilized the photograph within Australia on bus shelter ad shells.[144] It had never used the advertisement in the United States, nor had it posted the ad to the Internet.[145] Because the defendant had never directed any of its conduct towards the state of Texas, the American court held that it could not exercise personal jurisdiction over the defendant.[146]

This decision effectively left Chang without a substantive remedy. For one thing, she was an individual and a teenager without the wherewithal to sue the defendants in Australia. Perhaps more significantly, Australia does not have the same privacy torts available to plaintiffs as the United States. In the United States, Chang could have claimed misappropriation of her personal image under the misappropriation limb of privacy tort law.[147] The misappropriation tort provides a remedy to a plaintiff where a defendant has made an unauthorized commercial use of her name or likeness.[148] There is no similar tort in Australia, even if Chang had the wherewithal to litigate there. Thus, the effective resolution of the dispute for lack of jurisdiction foreclosed the possibility of a substantive discussion of the legal nature of privacy rights and expectations in the global online arena.

There may in fact be nothing wrong with the ultimate holding in *Chang*.

---

[142] 2009 U.S. Dist. LEXIS 3051 (2009).

[143] *Id.*, at 1 (Plaintiffs Susan Chang as next friend of Alison Chang, a minor … sued defendant Virgin Mobile Pty Ltd., an Australian-based company, in Texas state court on claims for invasion of privacy, libel, breach of contract, and copyright infringement based on Virgin Australia's use of an image of Alison … in its 'Are You With Us or What' advertising campaign ….).

[144] *Id.*, at 4 ("The advertisement was placed on bus shelter ad shells in major metropolitan areas in Australia. Virgin Australia never distributed the advertisement incorporating Alison's image in the United States, including Texas, and it never posted the photograph on its website or on any other website.")

[145] *Id.*

[146] *Id.*, at 26 ("Because none of the … contacts on which plaintiffs rely establishes sufficient minimum contacts between Virgin Australia and the state of Texas, the court cannot constitutionally exercise personal jurisdiction over Virgin Australia.")

[147] Restatement 2d of Torts, § 652C (One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.")

[148] *Id.*

If Texas is not the correct forum for litigation, then Chang is out of luck. Too readily allowing plaintiffs to sue in their home jurisdictions in Internet cases, as noted above, may impose insurmountable burdens on defendants and hence on online speech more generally.

However, *Chang* is far from the only Internet case that has been effectively resolved by a jurisdictional inquiry either because the plaintiff could not afford to sue in the defendant's jurisdiction or because the plaintiff did not have an effective claim under the defendant's law. Many Internet cases have historically been effectively resolved at the jurisdiction determination stage, or have used the jurisdictional inquiry as a testing ground for considering the merits of the case.[149] The proportion of Internet cases raising jurisdictional issues is likely to be higher than the proportion of non-Internet cases. Thus, Internet law creates greater risks of jurisdictional inquiries detracting from the opportunity to debate and develop substantive legal rules.

A reconceptualized cyberlaw field could contribute a more systematic *ex ante* approach to the development and application of jurisdictional principles in Internet-related cases. The ability to more quickly, efficiently, and predictably resolve jurisdictional problems would allow greater focus on developing more meaningful substantive rules for online conduct. Of course, jurisdictional issues both online and offline are often extremely difficult to resolve. Nevertheless, the ability to focus specifically on cyberspace-related jurisdictional problems within a more unified theoretical framework is likely to assist in more principled and predictable legal developments.

IV. CONCLUSIONS

Rather than being dismissed as a cyber 'law of the horse', cyberlaw is much more effectively characterized as a law of the intermediated information exchange with global dimensions. There is a pressing need to recognize a body of legal theory within which to debate the role of Internet intermediaries within the global information economy. Across a variety of fields – intellectual property, defamation, privacy, fraud etc – Internet intermediaries face common problems. Yet, there is currently no obvious theoretical space within to debate these issues.

---

[149] For example, in *Cable News Network v CNNews.Com*, 162 F. Supp. 2d 484 (E.D. Va. 2001), the court avoided substantive issues relating to cybersquatting by effectively resolving the dispute on jurisdictional grounds.

Cyberlaw scholars are overly focused on subject classifications of disputes and fail to draw together common threads relating to Internet intermediaries in relation to issues such as balancing the need to encourage online innovation against the need to prevent online wrongs. Thus, the pastiche of legislation and caselaw that has developed over the past fifteen years or so has been inconsistent depending on the specific subject matter at hand in a particular context.

The cyberlaw of the future should revolve around detailed analysis of the legal responsibilities of Internet intermediaries in many contexts. It should also incorporate jurisdictional considerations to ensure that the development of substantive legal principles is not hindered by overemphasis on procedural questions that could be more readily answered through development of clearer *ex ante* rules.

Refocusing the cyberlaw field on the global nature of the conflicts and the central role of online intermediaries will bring forth a more cohesive and predictable set of rules to govern online conduct. Once the legal rules are more clearly delineated in terms of ascertaining the substantive legal rights and obligations of intermediaries, the law can turn to other important issues of cyberspace regulation, such as: (a) ensuring conformity of laws with emerging online norms; (b) ensuring appropriate remedies for online harms; and, (c) creating appropriate liability rules for closed versus open service networks.[150] However, until a theoretical framework emerges within which to debate these issues, we are stuck with piecemeal and fragmented consideration of the legal role of online intermediaries within disparate subjects such as intellectual property, defamation, privacy, and fraud. It is time to reconceptualize the cyberlaw field with respect to what is truly unique about it – the fact that it governs global communications intermediated by one or more third parties.

[150] See *supra* note 31 for a discussion of the distinction between closed and open online networks.