September 2014

Cyberlaw 2.0

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

CYBERLAW 2.0

Jacqueline D. Lipton[*]

Abstract

In the early days of the Internet, Judge Frank Easterbrook famously dismissed the idea of an emerging field of cyberspace law as akin to a "law of the horse"— a pastiche of unrelated legal principles tied together only by virtue of applying to the Internet, having no unifying principles that would teach us anything meaningful. This article revisits Easterbrook's assertions with the benefit of hindsight. It suggests that subsequent case law and legislative developments in fact do support a distinct cyberlaw field. It introduces the novel argument that cyberlaw is a global "law of the intermediated information exchange." In other words, online law is unified by the fact that everything that occurs in cyberspace is an information exchange intermediated by one or more third parties - search engines, social networks, Internet Services Providers etc. Thus, cyberlaw is essentially about regulating communications amongst individuals, and apportioning liability between communicators and those who facilitate communication. Accepting this premise, one can identify a foundation – and set of unifying principles - for the field. This article advocates building up from this foundation to facilitate the development of a more cohesive, systematic and predictable set of rules for online governance.

INTRODUCTION

Law students in the 1990s flocked to enroll in new courses described variously as Internet law, cyberspace law, cyberlaw, and information law,[1]

[*] 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 Dean Lawrence Mitchell, Professor Nancy Kim, and Professor Cassandra Robertson for comments on an earlier draft of this article. All mistakes and omissions are, of course, my own.

[1] RAYMOND KU and JACQUELINE LIPTON, CYBERSPACE LAW: CASES AND MATERIALS, 16-17 (3 ed, 2010) ("The study of cyberspace law is … the study of the regulation of information in a world interlinked and mediated by computer networks …. In other words, the study of cyberspace law is the study of whether traditionally separate substantive laws that dealt with information should give way to a new overarching category of information law."); Jacqueline Lipton, *A Framework for Information Law and Policy*, 82 OREGON LAW REVIEW 695 (2003) (describing similiarities and differences between recognizing

despite criticisms that these courses were nothing more than a cyberspace "law of the horse".[2] Judge Frank Easterbrook had famously argued in 1996 that examination of property rights in cyberspace was no more than a survey of disparate legal principles related only by the fact that they were applied to the Internet.[3] He likened cyberspace law to a "law of the horse" on the basis that that field would include various principles of tort, contract and environmental law related only by the fact that they were applied to horses.[4] There would be no distinct unifying principles grounding the endeavor that would illuminate our thinking about the law more generally.[5]

Despite these criticisms, cyberlaw courses continue to be taught in law schools around the world.[6] Although the contours of the field have remained amorphous, the idea of cyberlaw has resonated with a large group of legal scholars.[7] This article questions why cyberlaw has maintained its traction despite Easterbrook's criticisms, and examines whether there may, in fact, be a unifying set of principles that underlie the field. In particular, the article takes advantage of the years of judicial and legislative developments since Easterbrook's comments to consider whether more than a decade of legal development now supports the field. In the author's view, new developments not only support the existence of a cyberlaw field, but more importantly require a re-organization of the field to better encapsulate what is unique and unifying about it.

It is easy to miss what is unifying about cyberlaw because the relevant principles appear in different guises across a variety of legal fields, notably

---

"cyberlaw" and "information law" as distinct fields of study).

[2] See, for example, Frank Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996) (famously arguing that cyberspace law amounted to nothing more than a "law of the horse").

[3] KU and LIPTON, *supra* note 1, at 16 (explaining the "law of the horse" metaphor as suggesting that "Internet law has no truly distinct value aside from being one of many potential areas for applying every legal discipline from antitrust to zoning law" to the Internet).

[4] Easterbrook, *supra* note 2, at 207 ("the best way to learn the law applicable to specialized endeavors is to study general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on 'The Law of the Horse' is doomed to be shallow and to miss unifying principles").

[5] *Id.*

[6] See, for example, Jessica Litman, List of Cyberlaw Syllabi (available at http://www-personal.umich.edu/~jdlitman/classes/cyber/courses.html, last viewed on August 1, 2011).

[7] So much so, in fact, that 2011 saw the inception of a new annual works in progress conference dedicated to the cyberlaw field: http://law.scu.edu/hightech/internet-law-scholarship.cfm, last viewed on August 8, 2011.

torts, intellectual property law, constitutional law, and criminal law. The aim of this article is to draw key principles together to make the case for cyberlaw. The author argues that the main concepts around which cyberlaw might be arranged are: examining Internet intermediary liability for the wrongful conduct of others; identifying appropriate behavioral norms specific to online interactions; addressing jurisdictional challenges specific to the Internet context; identifying a concept of compensable *harm* in online disputes; and, as a corollary, quantifying *damages* for online wrongs.

These concepts derive from the underlying nature of the Internet: a global communications medium where communications are facilitated by intermediaries such as Internet Service Providers (ISPs), virtual world operators, online gaming platforms, social network operators, web-hosting services, search engines, and payments systems. What is unique about cyberlaw is that it is the law of the *intermediated information exchange*. The unifying features of cyberlaw relate to the fact that the field deals purely with *information exchanges* and that those exchanges are always facilitated by one or more *intermediaries*. Nothing happens online that is not a form of intermediated information exchange. Thus, the cyberlaw field must focus, as no other field has before, on developing principles that regulate how we communicate with each other globally in a variety of spheres of activity (social, commercial, artistic) utilizing intermediated digital technologies.

Part I provides a history of cyberlaw, including prominent critiques of the field. Part II focuses on Internet intermediary liability as a central tenet of cyberlaw. If cyberlaw is a law of the intermediated information exchange, the role of the intermediary must take on paramount importance. Part III addresses online behavioral norms. Cyberspace interactions involve different behavioral norms from those that have developed in the physical world and the law must come to reflect those norms.[8] Part IV turns to

[8] Just as "real world" tort law embodies reasonableness standards (such as the omniscient "reasonable person") cyberlaw too should develop notions of reasonable online conduct. However, because cyberspace interactions are pure information exchanges and do not involve physical conduct, reasonableness standards online cannot be based on spatial analogs drawn from the physical world. Privacy law, for example, has developed the concept of a "reasonable expectation of privacy" based on physical doors, walls, fences, and locks: DANIEL SOLOVE, UNDERSTANDING PRIVACY, 71-74 (2008) (describing the concept of a "reasonable expectation of privacy" as it has developed in American Fourth Amendment jurisprudence and privacy tort law) [hereinafter, *Understanding Privacy*]. This kind of "reasonableness" standard does not easily translate to cyberspace: Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARVARD JOURNAL OF LAW AND TECHNOLOGY 1, 4 (2007) (noting that traditional American conceptions of

jurisdictional questions. It examines the extent to which cyberlaw has required, or may yet require, a reconsideration of traditional private international law principles. It suggests that the global nature of the Internet – requiring a jurisdictional inquiry in a majority of cases – may lead to a situation where jurisdictional boundaries serve routinely to bar substantive relief to individual litigants. The author argues that more predictable *ex ante* jurisdictional rules must be developed to allow for more effective determination of substantive legal rights online.[9] If the jurisdictional hurdles can be dealt with more effectively and predictably, judges will be able to focus more fully on developing substantive rights and remedies.

Part V examines the nature of harms and remedies online. Online harms deriving from information exchanges are predominantly reputational, emotional, and psychological. These kinds of harms are notably different to the kinds of harms traditionally addressed by, say, tort and intellectual property laws. Traditional laws have focused much more on economic harms often deriving from physical damages to a person or her property. The cyberlaw field needs to develop ways to identify and address harms arising from pure information exchanges and to effectively remedy those harms.

The author concludes in Part VI that by drawing together the issues discussed in Parts II to V, a clearer picture of a distinct cyberlaw field emerges, with its own set of unifying principles. While parties would continue to litigate disputes under existing laws, development of a cyberlaw field alongside those existing fields would facilitate the creation of more cohesive, harmonized, and predictable rules for Internet governance.

I. A BRIEF HISTORY OF CYBERSPACE

A. In The Beginning…

Most of us can no longer conceive of a world without the Internet, let alone the various handheld wireless devices – smart phones, iPads, and the like - enabling connectivity from virtually anywhere around the globe. Nevertheless, the previous generation – including many of today's law professors - witnessed the birth of the Internet. Some of us still remember a time when there was no cyberlaw course in the law school curriculum.

---

privacy do not translate well to the "spaceless" environment of the Internet).

[9] Cassandra Robertson, *The Inextricable Merits Problem in Personal Jurisdiction*, (draft on file with the author) (arguing for a clearer *ex ante* jurisdictional rule in Internet defamation cases).

Variously entitled cyberlaw, cyberspace law, or Internet law, these courses are now a staple of most upper level curricula.

Despite the apparent permanence of cyberlaw courses, no one has yet accurately explained the nature of the field. Cyberlaw casebooks focus variously on topics such as copyright and trademark law, First Amendment, privacy, jurisdictional problems, electronic contracting, regulatory competence of domestic legislatures, and private ordering.[10]

It was in the face of the uncertainties surrounding the appropriate boundaries of the field that Judge Frank Easterbrook made his famous "law of the horse" comments at the University of Chicago.[11] In remarks prepared following an invitation to comment on property law in cyberspace, Judge Easterbrook cited comments made by Dean Gerhard Casper, ex dean of the University of Chicago School of Law, to the effect that Casper was proud that Chicago did not offer a course in "the law of the horse".[12]

In likening cyberspace law to a "law of the horse", Easterbrook echoed Casper's concerns. Easterbrook noted specifically that courses involving the cross-sterilization of several fields, such as law and technology, tended to offer the worst of both worlds.[13] They would be doomed to be taught by professors who "knew little about either field".[14] Easterbrook also opined that the most effective way to learn laws as they might apply to specialized endeavors is to study rules of general application.[15] Otherwise, any new field that emerged would lack unifying principles that might illuminate anything meaningful about the law more generally.[16]

Easterbrook's comments were met with a variety of responses defending the existence of cyberspace law from a number of conceptual perspectives. In a well known response to Easterbrook in the Harvard Law Review, Professor Lawrence Lessig argued that cyberlaw did, in fact, illuminate the

---

[10] See, for example, KU and LIPTON, *supra* note 1; MARK LEMLEY, PETER MENELL, ROBERT MERGES and PAMELA SAMUELSON, SOFTWARE AND INTERNET LAW (3 ed, 2006); GERALD R. FERRERA, STEPHEN D. LICHTENSTEIN, MARGO E. K. REDER, ROBERT BIRD and WILLIAM T. SCHIANO, CYBERLAW: TEXT AND CASES (2003); PETER MAGGS, JOHN SOMA and JAMES SPROWL, INTERNET AND COMPUTER LAW: CASES – COMMENTS – QUESTIONS (2ed, 2005).

[11] Easterbrook, *supra* note 2.

[12] *Id*., at 207.

[13] *Id.*

[14] *Id.*

[15] *Id.*

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

entire law, although not in the way described by Easterbrook.[17] Lessig acknowledged that cyberlaw might be conceived as a series of disconnected tort, contract, and intellectual property problems as a matter of substance.[18] However, he noted that: "there is an important general point that comes from thinking in particular about how law and cyberspace connect."[19] 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.[20]

Lessig utilized this insight as a springboard for his well-known work that examines the application of a number of regulatory modalities in both real space and in cyberspace. These modalities include law, social norms, markets, and architecture.[21] In his subsequent work, he has focused on the significance of system architecture, or software code, as the key regulatory modality for cyberspace.[22] Lessig's insight was that online behavior can be more or less completely and almost perfectly regulated by software code to an extent that the law could never achieve.[23]

Professor Raymond Ku took a slightly different approach to Easterbrook's concerns. While agreeing that one could regard cyberspace law as an intersection of a variety of different fields, Ku suggested that cyberspace law nevertheless does potentially "illuminate the entire law". [24]

---

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

[18] *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.")

[19] *Id.*

[20] *Id.*

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

[22] LAWRENCE LESSIG, CODE: VERSION 2.0 (2 ed, 2006) [hereinafter, CODE 2.0].

[23] Lessig, *What Cyberlaw Might Teach*, *supra* note 17, 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").

[24] Raymond Ku, *Foreword: A Brave New Cyberworld?*, 22 T. JEFFERSON L. REV 125, 127-128 (2000) ("As lawyers, judges, lawmakers, and scholars, we have an obligation to

Ku argued that it was imperative to apply real world laws online to see whether they were effective in that context. In so doing, the opportunity would arise to question fundamental legal principles as they have applied in the pre-Internet world.[25]

Despite the flurry of heated debate in the immediate wake of Easterbrook's comments, no one has seriously tackled questions about the fundamental nature of cyberlaw since the 1990s. Cyberlaw courses and casebooks continue to comprise piecemeal collections of legal principles – tort, contract, antitrust, intellectual property, constitutional law, etc. – as applied to the Internet. An examination of these current approaches to cyberlaw suggests that Easterbrook's concerns may have been well-founded.

No serious attempts have been made to identify and develop what may be unique about cyberlaw as a field of study since the 1990s. 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.[26] Another ongoing debate has focused on the regulatory competence of domestic governments over the Internet.[27] This debate ultimately led to the coining of the term "cyberspace exceptionalism," referring to the view that traditional domestic governments cannot meaningfully regulate cyberspace and that new systems of regulation

---

examine the law and cyberspace and to take part in the discourse on how our cyberworld will be regulated. While Judge Easterbrook is clearly right that this effort requires a general understanding of the laws of intellectual property, antitrust, or the First Amendment, I disagree with his conclusion that the study of cyberspace does not 'illuminate the entire law.'")

[25] *Id*., at 129 ("pioneering our cyberworld and determining the rules and laws that will govern, forces us to examine our pre-cyberworld rules as well as our commitment to the values that form the foundation for those laws").

[26] 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).

[27] 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).

must be developed for online conduct.[28]

Important as these subsequent debates unquestionably have been, they do not answer fundamental questions about the nature and contours of cyberlaw as a legal field. The way in which one approaches these other debates will impact the answers to some of the questions posed in this article. However, the focus of this discussion is on examining legal developments in cyberspace to tease out unifying threads that will enable us to map the contours of a distinct cyberlaw field.

B. The Nature of Cyberspace: Global Intermediated Information Exchange

The key features of the Internet that effectively form the cornerstones of the following discussion are the fact that: (a) all online conduct involves information exchange;[29] (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 go online or participate in online interactions without contracting with an ISP. Once online, the Internet experience is only meaningful when one engages in interactions such as online games, social networks, virtual worlds, electronic commerce, or searching for items of interest. All of these interactions involve intermediaries such as Facebook,[30] Flickr,[31] MySpace,[32] Shutterfly,[33] Amazon,[34] Google[35] etc.

---

[28] David Post, *Governing Cyberspace: Law*, 24 SANTA CLARA COMPUTER & HIGH TECH. L.J. 883 (2008) (contrasting cyberspace "exceptionalists" and cyberspace "unexceptionalist" with respect to their respective views about cyberspace regulation)

[29] 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).

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

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

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

[33] 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.

[34] 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.

Internet intermediaries appear at many points within the online experience, and they are necessary to enable all online experiences.

Online interactions are basically exchanges of information amongst individuals. The information exchanges may be very sophisticated, such as the avatars[36] in Second Life[37] interacting with each other within a virtual environment. However, no physical interactions ever take place between real people online. Even cybersex – the cyberspace analog of the most intimate of physical acts - does not involve actual physical contact between individuals.

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. To understand cyberlaw, one must understand the nature of the relationships between principal actors in an information exchange, as well as their relationships to those who facilitate their exchange. One must also recognize harms and damages that result from *communications* as opposed to physical conduct. Online harms are likely to implicate a victim's reputation and mental or emotional well-being, rather than causing physical or economic damage.

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, it is likely that the prominence of jurisdictional issues may detract from the development of substantive legal rules. An associated challenge in recognizing the bounds of cyberlaw is to identify appropriate behavioral norms online, and to appreciate the extent to which online norms differ from norms of the physical world. Where individual actors are confronted with a computer screen rather than a physical person,

---

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

[36] Second Life, Definition of Avatar ("In a virtual world, an avatar is a digital persona that you can create and customize.", see http://secondlife.com/whatis/avatar/?lang=en-US, last viewed on August 1, 2011. Urban Dictionary defines "avatar" as: "An icon which represents a user in a virtual reality/Internet setting, currently attempted with varying success. The term is adopted from Neal Stephenson." See http://www.urbandictionary.com/define.php?term=avatar, last viewed on August 1, 2011.

[37] Wikipedia, Second Life ("Second Life is an online virtual world developed by Linden Lab which was launched on June 23, 2003."), see http://en.wikipedia.org/wiki/Second_Life, last viewed on August 1, 2011.

those actors are bound to behave differently – and may be expected to behave differently – than they would in a physical interaction.[38] The distinctive qualities of cyberlaw that have been identified in this Part are fleshed out in Parts II to V. The initial focus in Part II is on the key role of Internet intermediaries to the development of a meaningful cyberlaw field.

II. INTERNET INTERMEDIARIES: THE LAW OF THE MIDDLEMEN

A. With Great Power Comes Great Responsibility

Internet intermediaries are the backbone of Internet interactions. 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 concern and scrutiny.[39]

Defining the role of Internet intermediaries in terms of their legal responsibilities towards others must be a central focus of cyberlaw. The power of intermediaries is not restricted to their ability to control access to their services through passwords and other encryption technologies. Intermediaries are also able to control the user experience by controlling the underlying software code.[40] An avatar in Second Life can only be – and do - what the software will support. Initially, Second Life did not provide skin

---

[38] Lyrissa Barnett Lidsky and Thomas Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 NOTRE DAME L REV 1537, 1575 (2007) ("Studies show that even when an Internet user is *not* anonymous and knows the recipient of his e-mail message, the speaker is more likely to be disinhibited when engaged in 'computer mediated communication' than in other types of communications. The technology separates the speaker from the immediate consequences of her speech, perhaps (falsely) lulling her to believe that there will be no consequences. Since the Internet magnifies the number of anonymous speakers, it also magnifies the likelihood of false and abusive speech."); ROBIN BARNES, OUTRAGEOUS INVASIONS: CELEBRITIES' PRIVATE LIVES, MEDIA, AND THE LAW, 35 (2010) ("Mass electronic communication eliminates the self-censorship that normally occurs when dealing with an individual or communicating face-to-face.")

[39] 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).

[40] See *supra* note 22.

colors for avatars outside the Caucasian range. The game now supports the creation of alternative tones – or "skins"[41] - 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.

This Part considers the role of Internet intermediaries, and outlines some of the key issues about intermediary liability and responsibility that should be central to cyberlaw. It considers the extent to which intermediaries are appropriately held liable for direct infringements of legal rights in areas such as defamation, privacy, copyright, and trademark law. It also examines the challenging questions of where to set the boundaries for secondary liability of intermediaries with respect to wrongs committed by others. Finally, it examines other obligations that may be owed by intermediaries to victims of online wrongs, such as the obligation to identify primary wrongdoers for the purposes of legal proceedings.

B. Direct Versus Indirect Liability for Online Wrongs

The power and prominence of intermediaries underscore the importance of appropriately regulating these entities. 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 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 either as a direct participant (primary infringer) or as a facilitator (secondary infringer).

While questions of intermediary liability comprise many pages in most cyberlaw casebooks, these pages tend to be scattered throughout different chapters. Questions about intermediary liability for copyright infringement will be discussed in a chapter about copyright law, while intermediary liability for defamation and privacy will typically be discussed in a free speech, privacy, or general tort chapter. While one aim of this article is to support a cyberlaw field, another important goal is to re-organize the field to better reflect legal developments over the last decade or so. It may make sense in the future for discussions of intermediary liability to be considered together across all relevant fields of law – copyright, trademark,

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

defamation, privacy, bullying, harassment etc. This would allow synergies between existing fields to be identified. It would further facilitate the development of more meaningful, harmonized, and predictable legal rules.

It is increasingly difficult to ascertain whether an intermediary should be held primarily, or rather secondarily, liable for many online wrongs. Where a wrong is committed in the physical world – such as theft, conversion, negligence, or battery – the identity of the primary wrongdoer is usually readily apparent, and it is usually not an intermediary. Even if a third party intermediary facilitates the wrong, the actual wrongdoer is typically easy to distinguish from that third party. If I steal from you and deposit the proceeds of the theft 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 or middleman – is not the primary wrongdoer. The bank might be at most complicit in my primary wrongdoing depending on its level of knowledge of, or participation in, my wrongful conduct.

Online, however, it is often difficult to discern who is most appropriately described as the primary wrongdoer. In a recent trademark case involving keyword advertising, for example, it was not clear whether the Netscape search engine should be regarded as a primary or rather a secondary infringer.[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]

The plaintiff in this case – Playboy Enterprises – complained that Netscape had included its trademarked terms "playboy" and "playmate" for

---

[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.")

keying advertisements related to sex and adult entertainment.[46] It was not clear on the face of some of the resulting advertisements whether they were officially related to the plaintiff's business.[47] Thus, the Internet user clicking on the ad could potentially be confused as to whether it was dealing with Playboy or an unaffiliated entity providing similar services. A successful infringement action requires consumers of a product or service to be confused about the source of that product or service.[48] Playboy thus claimed infringement with respect to the confusing advertisements keyed to the terms "playboy" and "playmate".

While ultimately holding Netscape liable for infringement, the court was unsure about whether Netscape was a direct infringer or a secondary infringer.[49] In many ways, secondary liability for Internet intermediaries makes the most sense. Intermediaries, by definition, are third parties who facilitate activities between principal actors. If one of the principals commits a wrong, then it would be logical to suppose that the intermediary would generally be at most secondarily liable.

However, online the lines are blurred largely because the intermediaries control the software code. If Netscape codes its keyword advertising software in a certain way and advertisers choose from keywords pre-selected by Netscape, should Netscape face primary liability because of its control over the functionality of the system? The *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 easily 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

---

[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 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.")

because of its choice of the keywords it coded into the system.

While the basis of Netscape's liability did not have much practical impact in this decision, there will be cases in which determination of the nature of an intermediary's liability will have a significant impact on the outcome. In the more recent *Cartoon Network* case involving copyright infringement claims the court considered whether the provider of a digital video recorder (DVR) was primarily or secondarily liable for content copied to its servers at the request of its customers.[51] This issue simply could not have arisen in the pre-digital world of video recording. In the days of Betamax and VHS recorders, it was clear that any primary infringements – unauthorized copies – were made by owners of video recorders. The providers of the copying technology were not involved in the primary infringements. They did not decide which programs were recorded, when, or how often. They did not even know what programs were being recorded by their customers. They merely provided the technology that enabled the copying. The Supreme Court in 1984 considered whether Sony as the manufacturer of the Betamax video tape recorder might be held liable for infringements of copyrighted works carried out by its customers. However, it could only potentially have been *secondarily* liable as Sony itself did not conduct any copying.[52]

New digital technology enables the copying process to occur remotely over a network. The DVR service in *Cartoon Network* mimicked the functionality of an old-fashioned analog video recorder, but in practice worked quite differently. As with a set-top video recorder, the DVR service provided by the defendant – Cablevision – to its customers allowed 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.[53] Thus, Cablevision itself physically made the infringing copies of protected television programs, but at its customers' request.[54]

The *Cartoon Network* court held that Cablevision was not a direct infringer of the defendants' copyrights.[55] According to the court, if there

---

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

[52] *Sony v Universal City Studios*, 464 U.S. 417 (1984) (holding that manufacturers of Betamax video recorders were not liable for copying conducted by their customers as the customers were making fair uses of the copyrighted material).

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

[54] *Id*

[55] *Id*., at 133 ("We conclude only that on the facts of this case, copies produced by the

was any infringement, it was the users of the service who effectively made the copies by ordering Cablevision's servers to record them.[56] 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.[57] This practice was labeled "time shifting" and was considered by a majority of the Court to be a fair use of the copyrighted work.[58] Assuming that Cablevision's customers were largely engaged in time-shifting, there would be no primary infringement for which Cablevision could be secondarily liable.[59]

While this reasoning makes sense in practice, the *Cartoon Network* court went to great lengths to avoid holding Cablevision liable as a direct infringer. As Cablevision in fact did make the actual copies of the protected works, and as copyright infringement is a strict liability wrong,[60] it would seem on first impression that Cablevision should have been held primarily liable. It was only by reading a volition requirement into copyright infringement that the court was able to avoid this result.[61] Following an

---

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.")

[56] *Id.*

[57] *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.")

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

[59] *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.")

[60] 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").

[61] *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 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

earlier Internet intermediary precedent,[62] the court started chipping away at the strict liability basis of copyright infringement in order to reach the desired result.

Identifying the nature of an intermediary's liability for online wrongs raises a number of important challenges. Lawmakers must be aware of the need to check the power held by online gatekeepers when wrongs are committed, but at the same time avoid over-regulating and thereby chilling technological innovation. The intermediary's power stems from the nature of the Internet as a mode of intermediated information exchange. Intermediaries control access to information as well as the code that enables users to engage in online activities.

However, that power in itself does not always justify the imposition of primary liability. As in the *Cartoon Network* case, sometimes a court will promote technological innovation by avoiding a finding of primary liability. Questions of primary versus secondary liability for intermediaries come up again and again in different contexts online.[63] This fact suggests a need to focus on the legal responsibilities of intermediaries within a cohesive cyberlaw field, rather than in disparate areas of the law such as copyright, trademark, defamation, and privacy.

---

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*].

[62] *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).

[63] *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. Intermediary Secondary Liability

Even within the context of secondary liability, lawmakers face challenges about the appropriate scope of intermediary liability for online wrongs committed by others. 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.[64] Courts were asked whether providers of such forums could be held liable for communications posted by their members and, if so, on what basis.[65] The most common claims in the late 1990s related to defamation and copyright infringement.[66]

In the absence of a unified cyberlaw field, courts considered ISP liability purely from the point of view of the field of law from which the claim arose: defamation or copyright. Little thought was given to the overarching impact of the principles of intermediary liability on the development of online law more generally. In other words, lawmakers may have missed significant critical points in the development of Internet law to ensure a systematic consideration of principles of Internet intermediary liability and to develop coherent principles to guide intermediaries in their future conduct. 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

---

[64] *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)

[65] *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).

[66] See *supra*, note 64.

posted.[67] This soon proved problematic because it effectively penalized ISPs who were attempting to "do the right thing" and censor inappropriate conduct. The more active the ISP was in, say, protecting children from harmful material, the more likely it would be to attract legal liability.[68] ISPs that turned a blind eye to communications they facilitated were more likely to escape legal liability than those that were more pro-active about monitoring content.[69]

Congress eventually intervened, enacting § 230 of the Communications Decency Act (CDA). This section, in relevant part, provides that: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[70] Courts interpreted this provision as almost a blanket immunity for ISPs for any defamatory comments posted by others.[71] ISPs were exempted from liability even in situations where they were complicit in the posting of defamatory or harmful content. 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 at least occasionally defamatory.[72] 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.[73] To date, ISPs have only been held liable as information content providers under § 230 where they have

---

[67] *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).

[68] *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).

[69] *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.")

[70] 47 U.S.C. § 230(c)(1).

[71] 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.'")

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

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

actually *written* the relevant content themselves,[74] rather than having contracted with another to write it.

The current position on ISP liability for defamation and other harmful speech 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 speech forums should be held liable for those infringements.[75] 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.[76]

Congress enacted the Online Copyright Infringement Liability Limitation Act (OCILLA) as part of the Digital Millennium Copyright Act of 1998. OCILLA provides a safe harbor for direct ISP liability 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.[77] The statute also exempts ISPs from secondary 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.[78]

The ISP safe harbors for defamation and copyright were enacted around the same time.[79] However, the respective statutes take quite different approaches. This result is not surprising as 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.[80] Both statutes would have been incredibly challenging to draft, particularly in the early days of the Internet when it

---

[74] *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).

[75] *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).

[76] 17 U.S.C. § 512.

[77] 17 U.S.C. § 512(a).

[78] 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).

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

[80] Lukmire, *supra* note 71, 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).

was unclear how relevant technologies would ultimately develop and how people would use them.

Nonetheless, there were significant commonalities between what the drafters were trying to do, 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 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 with no broader focus on the Internet's development more generally. This is where the acceptance of a cyberlaw field may have been helpful. It would have provided an obvious theoretical framework for discussions of important policy issues across disparate disciplines that raise significant commonalities online.

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 and is basically 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[81] and because OCILLA requires the claimant to give detailed notice to the ISP of a copyright claim.[82] Thus, it is arguably reasonable to hold ISPs liable for copyright infringement on the basis of notice but to largely 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 bona fides 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 an ISP up to potentially frivolous claims that cannot be easily verified. If the ISP is required to act on each claim by removing offending material – or at least investigating the merits - the resulting costs 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.[83]

---

[81] TEHRANIAN, *supra* note 60, at 98 (noting the necessity of registering copyrighted works in the United States in order to obtain meaningful judicial relief for infringement).

[82] 17 U.S.C. §(c)(3)(A).

[83] MARHSALL LEAFFER, UNDERSTANDING COPYRIGHT LAW, 273(5 ed, 2010) (noting

At the end of the day, the ISP is 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 rights that can be verified by the ISP, the ISP might legitimately be required to act to protect those interests. However, where the content involves pure speech which may damage a person's reputation, but which may or may not be defamatory, the ISP is not in as good a position to make a determination about the merits. Thus, Congress and the courts effectively made the decision to exempt the ISP from most liability in the defamation area, and to promote free speech and technological innovation. This result puts aggrieved parties in the position of having to sue the primary infringer - the person who actually wrote the allegedly defamatory content.

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 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.

A renewed focus on cyberlaw as a legitimate field would create a policy-oriented space for debates about commonalities between apparently disparate areas of law like defamation and copyright, as applied online. This would be a useful development particularly in the area of intermediary liability for content created or posted by others. There is an urgent need for a theoretical framework within which to engage in discussions of intermediary liability. New issues of intermediary liability are constantly arising, often requiring novel applications of legal principles.[84]

---

that registration of a copyright "confers prima facie evidence of the validity of the copyright").

[84] LOWE, *supra* note 39, 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

For example, in two recent cases, the Ninth Circuit considered the extent to which two different online service providers – the Google search engine in one case, and the Visa online payments system in the other – could be liable for copyright infringement.[85] The plaintiff in both cases was Perfect 10, a company that made its money from selling photos of nude models online.[86] 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 search results.[87] 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.[88] It should also be held secondarily liable for the infringements of the people who had actually made the illegal copies in the first place where the copies showed up in search results.[89] In the litigation against Visa, Perfect 10 claimed only secondary copyright infringement with respect to Visa enabling payments to companies that sold unauthorized reproductions of Perfect 10's protected photographs.[90]

With respect to the secondary liability claims, the court ultimately held

---

issues that could define both Google and the Internet of the future.")

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

[86] *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.")

[87] *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").

[88] *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).

[89] *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").

[90] *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.")

that Google could potentially be contributorily liable for the copyright infringements, but that there were factual matters to be reconsidered on remand.[91] 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.[92] 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."[93] 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.[94]

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".[95] In Judge Kozinski's view, without the payments systems, infringement would be almost impossible.[96] Clearly, there is room

---

[91] *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 …")

[92] *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.")

[93] *Id.*, at 797.

[94] *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.")

[95] *Id*., at 812.

[96] *Id.*("My colleagues recognize, as they must, that helping consumers locate

for disagreement as to where to draw the secondary liability line when it comes to Internet gatekeepers. While both the cases involving Perfect 10 were about copyright law, and did not impact other areas of law, the position of search engines and other online intermediaries is an unenviable one in many contexts.

While providing accessible and innovative services to enable individuals to interact more efficiently and effectively online, these 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 therefore 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. 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.[97]

Courts will continue to face questions of the secondary liability of online intermediaries in copyright and other areas of law. A broader cyberlaw-based perspective on these questions may ultimately be useful in creating laws that give more meaningful and predictable guidance to those providing online gateway services. Cyberlaw is the field in which this can be achieved. In recent years, scholars have made some headway in

---

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…")

[97] *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.")

examining relevant legal principles not from the point of view of specific legal field, but from the point of view of a particular Internet intermediary's perspective. This has occurred most prominently with respect to search engines. [98] Accepting a broader field of cyberlaw might prevent these debates from becoming piecemeal and degenerating into digital laws of the horse such as "the law of the search engine", "the law of the online social network," or "the law of virtual worlds".

D. Responsibilities to Unmask Online Wrongdoers

Internet intermediaries are often in the position of being the only entity 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.[99] Thus, victims of online wrongs cannot identify the person or persons engaging in harmful communications. Again, the power inherent in knowing people's true identities must come with responsibilities not to let those people abuse their anonymity.

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. Internet users may be loathe to communicate online for fear of being unmasked.[100] Intermediaries may also falter if they cannot protect their customers' privacy.[101] The requirement that intermediaries stand

---

[98] Viva Moffat, *Regulating Search*, 22 HARVARD JOURNAL OF LAW AND TECHNOLOGY 475 (2009); Greg Lastowka, *Google's Law*, 73 BROOKLYN L REV 1327 (2008); Oren Bracha and Frank Pasquale, *Federal Search Commission? Access, Fairness and Accountability in the Law of Search*, 93 CORNELL L REV 1129 (2008); James Grimmelman, *The Structure of Search Engine Law*, 93 IOWA L REV 1 (2007); Urs Gasser, *Regulating Search Engines: Taking Stock and Looking Ahead*, 8 YALE J L & TECH 201 (2006); Eric Goldman, *Search Engine Bias and The Rise of Search Engine Utopianism*, 8 YALE J L& TECH 188 (2006).

[99] Jacqueline Lipton, *Combating Cyber-Victimization*, ___ BERKELEY TECH. L.J. ___ (forthcoming, 2011) ("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.")

[100] 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)

[101] *Id*., at 1671 ("The Networld has an abundance of opportunities for full and

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[102] or a witness to an online wrong.[103] 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,[104] defamation,[105] trademark infringement,[106] and complaints about reputational harm.[107]

A broader look at these questions through the lens of Internet 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 a foundational part of the cyberlaw field. Intermediaries are necessary for all online transactions. No one can interact online without using at least one intermediary.

---

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.")

[102] *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).

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

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

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

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

[107] *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).

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. Along with this power come certain responsibilities. However, imposing legal responsibilities on intermediaries will generally come at a cost. The more duties legally imposed on intermediaries, the more likely the result will be a chilling of online innovation.

It is within the cyberlaw field that commentators and lawmakers will need to develop appropriate balances to impose obligations on intermediaries to an extent that will curtail online harm while preserving the vitality of online interaction. In order to develop this balance, it will be necessary to identify the scope of appropriate online behaviors more generally. Thus, another important aspect of the cyberlaw field must be an identification and explication of appropriate online norms of behavior.

III. CYBERNORMS

Cyberspace norms, their identification, and enforcement, often raise significantly different interests and dynamics than real space norms of behavior. Real space norms involve physical interactions between people and property while cyberspace norms involve communications over often great distances. In real space, people are confronted with other physical beings. Physical world interactions involve facial expressions, tone of voice, and physical appearance. It is often much more difficult to say to someone's face something that you would say behind her back, or that you would say anonymously or pseudonymously online.[108]

Real space laws have developed to reinforce – and simply to enforce – real space norms. Norms about protecting a zone of safety around a person, for example, are enforced through stalking and harassment laws.[109] The problem for cyberlaw is that many of the real world laws that protect individuals from harm do not apply meaningfully in cyberspace. The real space laws largely hinge on notions of physical space, personal safety and damage to people and property which do not always translate well to cyberspace.[110]

---

[108] See *supra* note 38.

[109] Lipton, *Combating Cyber-Victimization, supra* note 99, at ___ (citing examples of these laws).

[110] Sánchez Abril, *supra* note 8, at 4 ("In the absence of clear and relevant guidance, courts have resorted to intellectual shortcuts in their use of concepts of space, subject

The tort of conversion, for example, is fairly well circumscribed in physical space.[111] It is obvious in spatial terms whether or not someone has interfered with another person's physical property. But how might that play out in cyberspace? Can you meaningfully "convert" or "steal" another person's virtual or digital property? Most online property can exist in multiple places at the same time so taking (or copying) my digital property does not deprive me of my own access to it. This differs from the physical world where property is rivalrous: that is, it can only exist in one place at a time.[112] Thus, your taking of my property deprives me of the property. However, copying someone's digital widget creates a second widget and does not deprive the owner of the original widget or its use.[113] The taking may impact the value of the original widget, but not its very existence in the hands of the original owner. Few online assets are truly rivalrous in the same sense that physical property is rivalrous.

Even rivalrous online property can raise different legal issues from those arising in physical space. One example of rivalrous digital property is an Internet domain name.[114] A domain name can only be registered to one

---

matter, secrecy, and seclusion as necessary benchmarks for privacy protection. What were once mere indicators of privacy have become, in some instances, the extent of judicial inquiry. Problematically, these entrenched constructs are all related in one form or another to a pervasive consciousness of physical space, a concept that is no longer relevant in analyzing many modern online privacy harms.")

[111] Restatement 2d on Torts, § 222A(1) ("Conversion is an intentional exercise of dominion or control over a chattel which so seriously interferes with the right of another to control it that the actor may justly be required to pay the other the full value of the chattel.")

[112] Lawrence Solum, *Questioning Cultural Commons*, 95 CORNELL L. REV. 817, 822 ("'Rivalrousness' is a property of the consumption of a good. Consumption of a good is rivalrous if consumption by one individual X diminished the opportunity of other individuals, Y, Z, etc., to consume the good. Some goods are rivalrous because they are 'used up.' If I drink a glass of Heitz Martha's Vineyard, then you cannot drink that same glass of wine. If I set off a firecracker, you cannot set off the same firecracker. Other goods are rivalrous because of crowding effects. If I am using the free Internet terminal at the student lounge, then you cannot use the same time slice of the terminal - because only one person can sit in front of the screen at the same time.")

[113] The only effective way to actually deprive someone of her digital property is to *destroy* that property: for example, by deleting data from a protected server. The law has traditionally dealt with this kind of conduct by focusing on the *hardware* aspects of a digital system, rather than the content *per se*. See, for example, the Computer Fraud and Abuse Act: 18 U.S.C. § 1030 (dealing with hacking into computer systems and destroying data).

[114] JACQUELINE LIPTON, INTERNET DOMAIN NAMES, TRADEMARKS AND FREE SPEECH, 4 (2010) ("Domain names comprise a unique form of online asset. They are the closest Internet analogy to real property. This is because, unlike other forms of digital property,

person at a time.[115] Even so, it is not clear that real world notions of property interference apply meaningfully to domain names. While at least one court has held that a domain name is property capable of conversion,[116] the way in which the domain name was wrongfully appropriated was very different to an unauthorized taking of physical property. To convert a domain name, one must send a fraudulent request to the domain name registering authority to transfer the name.[117] It is not possible to simply "take" the name as one might take a car, a chair, or an apple. One must rely on an intermediary – in this case, a domain name registry – to effect the conversion. This again underlines the importance of intermediaries in the cyberworld.

Of course, real world laws have been developed to deal with information-based wrongs as well as physical wrongs. In other words, we already have laws that do not require physical property to exist for a wrong to have been committed. Defamation and privacy laws, for example, deal with harms caused by dissemination of damaging information about an individual. These torts, and their associated underlying behavioral norms, may be easier to apply online than property-based torts because they do not require physical harm to a person or property. Nevertheless, even these informational torts raise new challenges online.

Consider defamation law, for example. While defamation law in the physical world has typically dealt with professional media outlets publishing harmful information about individuals, online defamation can be quite different. As more individuals are publishing their own thoughts online, and defaming others in the process, the professional journalist is effectively replaced – or at least joined in the role of social commentator - by the amateur commentator.[118] With Web 2.0 technologies,[119] individuals

---

they are rivalrous. This means that one domain name can only be held by one person or entity at a time.")

[115] *Id.*

[116] *Kremen v Cohen*, 337 F. 3d 1024 (2003).

[117] Jacqueline Lipton, *Bad Faith in Cyberspace: Grounding Domain Name Theory in Trademark, Property and Restitution,* 23 HARVARD JOURNAL OF LAW AND TECHNOLOGY 447, 474 (2010) ("a transfer of a domain name is, in reality, a de-registration from the original registrant and re-registration to the new registrant, it is now treated routinely as a seamless transfer, as if the name was being handed directly from the original registrant to the new registrant.")

[118] ANDREW KEEN, THE CULT OF THE AMATEUR: HOW BLOGS, MYSPACE, YOUTUBE, AND THE REST OF TODAY'S USER-GENERATED MEDIA ARE DESTROYING OUR ECONOMY, OUR CULTURE, AND OUR VALUES (2007) (expressing concerns about the move from professional media to communal digital media); Larry Ribstein, *From Bricks to Pajamas: The Law and Economics of Amateur Journalism*, 48 WM AND MARY L. REV. 185 (2006)

easily share their thoughts about others on Twitter, blogs, and online social networks.

Naturally, when much of the world's social commentary is disseminated in this way, very different behavioral norms develop than when dissemination of information is predominantly in the hands of professional media conglomerates. Individual commentators are not bound by professional codes of ethics.[120] Individuals may hide behind a shield of anonymity more easily than professional journalists.[121] Further, individuals may simply not be as aware of the laws of defamation and privacy than professional media outlets. This is not to say that individual commentary should be prohibited or legally sanctioned more aggressively than professional commentary. Amateur or individual speech provides tremendous social benefits.[122] However, the norms of Web 2.0 informational transactions are significantly different from those that developed in the physical world. The existing defamation and privacy laws were simply not developed with these kinds of behavioral norms in mind.

Outside of the basic differences between online and offline norms are the practical difficulties of applying national defamation laws to online conduct because of the jurisdictional reach of particular laws and courts.[123] This is another reason why behavioral norms are increasingly important to online transactions. If norms can be identified and enforced by online communities, there is less need for victims of online wrongs to rely on law. In other words, laws can serve a signposting function about appropriate

---

(examining the rise of amateur journalism through blogging).

[119] LOWE, *supra* note 39, at 294 (defining "Web 2.0" as: "A term used to describe an evolving generation of a participatory Web. Web 2.0 describes the proliferation of interconnectivity and social interaction on the World Wide Web.")

[120] Ribstein, *supra* note 118, at 214 (noting that amateur journalists are typically not bound by codes of ethics and noting some of the advantages inherent of being free from such perceived constraints); KEEN, *supra* note 118, at 82 (noting lack of codes of ethics in amateur online journalism).

[121] KEEN, *supra* note 118, at 77 ("In traditional news media, there is no such thing as anonymity. Articles and op-eds run with bylines, holding reporters and contributors responsible for the content they create. This not only holds them to ethical standards, but also provides a level of assurance for the public; the writer is accountable for his or her reporting or opinions …. But in the anonymous world of the blogosphere there are no such assurances, creating a crisis of trust and confidence.")

[122] Ribstein, *supra* note 118, at 214 ("Even if it were feasible to develop norms for amateur journalists, it may not be desirable. An important social benefit of amateur journalists is that they are not subject to professional norms and constraints. In devising extralegal constraints, as with legal regulation, one must control the costs of amateur journalism in a way that does not sacrifice its benefits.")

[123] See Part IV, *infra*.

behavior[124] in contexts where intermediaries and online communities are already articulating and enforcing appropriate norms of behavior amongst themselves.[125]

Defamation is not the only area in which online norms may differ from the real space counterparts upon which existing laws were originally based. Other information-based torts raise challenges when applied online. Privacy laws, for example, rely to a significant extent on physical space metaphors. The notion of a "reasonable expectation of privacy" which arises in both criminal and tort-based privacy law is powerfully tied to notions of physical space.[126] One might be presumed to have a reasonable expectation of privacy behind a locked door but not in a public mall.

However, in cyberspace, it is much more difficult to delineate the boundaries of a reasonable expectation of privacy, particularly as so much digital media blurs the lines between our public and our private selves.[127] Sexting is an obvious example of conduct that may commence as a private and consensual act but may quickly escalate into the public domain depending on who ultimately gains possession of the images.[128] If a teenager engages in consensual sexual acts with a partner and agrees to a

---

[124] NEIL NETANEL, COPYRIGHT'S PARADOX, 104-105 (2008) ("[L]aw often serves an expressive or symbolic function above and beyond regulating or providing incentives for conduct. Antidiscrimination law, for example, may have symbolic importance beyond whatever discriminatory conduct it actually proscribes. In enacting and applying such law, Congress and the courts effectively express our society's official condemnation of discrimination based on race and various other classifications.")

[125] From the early days of the Internet, online communities have self-policed and enforced acceptable norms of behavior amongst themselves. See, for example, SHERRY TURKLE, LIFE ON THE SCREEN: IDENTITY IN THE AGE OF THE INTERNET, 251 (1995) (describing the "toading" of a virtual rapist in an early online environment, toading being the erasure of his character for his unacceptable behavior).

[126] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 8, at 74 (noting the difficulties inherent in determining reasonable expectations of privacy as privacy is effectively eroded through developing technologies such as data collection and digital cameras).

[127] BARNES, *supra* note 38, at 35-36 (noting how moves towards reality television and personal blogging blur the lines between public and private selves and make private individuals into instant celebrities).

[128] Elizabeth Eraker, *Stemming Sexting: Sensible Legal Approaches to Teenagers' Exchange of Self-Produced Pornography*, 25 BERKELEY TECH. L.J. 555, 557 (2010) ("Although sexting has been described as the modern equivalent of 'streaking,' new technologies dramatically enhance the consequences of this behavior. Camera-equipped phones allow permanent recording of images and instant dissemination to large numbers of recipients, transforming fleeting youthful indiscretions into lasting mistakes …. the term 'sexting' refers to the self-production and distribution by cell phone of sexually explicit images in the course of consensual, voluntary activity by teenagers").

video or picture memorializing the event, does that mean there should be no expectation of privacy from that point forward?

Certainly, one could argue that all modern teens with cellphone-cameras know that once an image is captured on the phone, it can be globally disseminated over the Internet at the push of a button. On this basis, it may be reasonable to differentiate this conduct from an old-fashioned physical photograph of a consensual sexual act. Even though the physical image may be shared with others, it cannot be as easily, quickly, cheaply, and globally disseminated at the push of a button. The hard copy photograph also lacks the permanence of an Internet distribution of a digital image. Once a hard copy photograph is destroyed, no one can view it anymore. However, once a digital image is disseminated online, there is no way to permanently eradicate it, even if the original image is deleted from where it was initially posted.[129]

Of course arguing about the importance of online norms runs the risk of suggesting that laws are irrelevant in cyberspace. Additionally, to the extent that one argues in favor of norm enforcement within a community, one potentially circles back to debates about whether cyberspace can – or should - be meaningfully regulated by national governments,[130] and whether law is the most appropriate form of regulation in cyberspace.[131] Emphasizing the importance of norms online does not necessarily mean that laws and national governments are irrelevant. Rather, it is important to consider norms as the basis of legal rules, while acknowledging that norms can be enforced outside of the law.

Even the earliest Internet communities developed ways to punish those who disregarded behavioral norms.[132] Norms of more recent online communities are often enforced through private online dispute resolution procedures that support express rules of the forum. Wikipedia and Second Life, for example, have each developed express rules of online behavior that are enforced by private mechanisms.[133] Legal rules based on cybernorms can also serve an important expressive function in helping us to identify

---

[129] Jacqueline Lipton, *"We, the Paparazzi": Developing a Privacy Paradigm for Digital Video,* 95 IOWA L. REV. 919, 977 (2010) (describing the impossibility of removing all iterations of a given image from the Internet).

[130] See *supra* note 27.

[131] See Lessig, *What the Law of the Horse Might Teach, supra* note 17.

[132] See TURKLE, *supra* note 125.

[133] Lipton, *Combating Cyber-Victimization, supra* note 99, at Part III.D.4 (describing approaches to industry self-regulation online).

appropriate dimensions of online behavior in particular contexts.[134]

The cyberlaw field provides a necessary framework within which to situate debates about the identification of online norms in a variety of fields, their divergence from physical world norms, and their relationship to legal rules. It provides commentators and lawmakers with a conceptual space within which to consider legal developments that reflect and reinforce appropriate norms of online behavior. Of course, one of the reasons that investigating norms is so important in cyberspace is that laws may have limited jurisdictional reach online. It is to those jurisdictional challenges that we now turn our attention.

IV. JURISDICTION

A. Cyberspace Conflicts: Jurisdiction and Enforcement

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.[135] 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 were cases where the defendant held 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.[136]

In the *Yahoo!* litigation, a French plaintiff successfully obtained a French court order to have Yahoo! enjoined from selling Nazi memorabilia in France.[137] Subsequently, Yahoo! took up the matter in California and attempted to obtain a declaration from the Californian courts that the French

---

[134] NETANEL, *supra* note 124.

[135] 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).

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

[137] *Id.*

order would not be enforced against Yahoo!'s assets in California.[138] To date, the Californian courts have refrained from giving a definitive answer to this question.[139] The Californian courts have been split on issues whether the case is ripe for a decision, and as to whether the Californian courts can exercise personal jurisdiction over the French organization.[140] The United States Supreme Court has denied certiorari,[141] so ultimately any decision made will be in a lower court in California.

Jurisdictional questions are not necessarily new to the Internet. However, the Internet raises new challenges for conflicts of law by its very nature. For one thing, 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,[142] early courts tended to consider the location of physical computer servers.[143] This approach led to random and unpredictable results because of the nature of the Internet. 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.[144] Thus, premising jurisdictional queries on electron flows is unlikely to lead to principled and predictable legal rules.

---

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

[139] *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.")

[140] *Id.*

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

[142] 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).

[143] 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).

[144] 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.")

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 effectively an online communication, and that communication is accessible globally, the purposeful availment inquiry is not very meaningful in practice. 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?[145]

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 in the past,[146] 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 defendant.[147] 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 fact that defendants would face such 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.[148] These concerns come into sharp

---

[145] *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).

[146] *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."); Robertson, *supra* note 9; *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).

[147] Robertson, *supra* note 9, at ___ (arguing that in the digital age, personal jurisdiction queries should be presumptively resolved in favor of the defendant).

[148] *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).

relief in situations where defendants are increasingly amateur journalists and social commentators who would not have the wherewithal to defend a proceeding in a foreign jurisdiction.[149]

While there are a number of counter-arguments to concerns about unfairness to defendants,[150] the point of this discussion is not to identify the correct rule on personal jurisdiction in cyberspace. Rather, it is to demonstrate that cyberspace raises distinct legal challenges that merit its treatment as a discrete legal field with its own set of unifying principles. One of those principles has to be the investigation of what factors differentiate cyberspace from physical space in the context of determining how to approach 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.

B. Jurisdiction Deterring Substantive Rights

The Internet may raise additional challenges related to basic jurisdictional questions. 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 greater number of jurisdictional issues in cyberlaw as compared with physical world cases, a greater proportion of cyberspace law cases might be disposed of at the

---

[149] Robertson, *supra* note 9, at ___ (noting that many publishers online are now private individuals and it would be unfair to presume their amenability to foreign jurisdiction).

[150] *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 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").

jurisdictional stage without ever getting to a determination of the parties' substantive rights and obligations. 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 jurisdictional questions in particular cases, 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 is *Chang v Virgin Mobile*.[151] 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.[152] 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.[153] It had never used the advertisement in the United States, nor had it posted the ad to the Internet.[154] 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.[155]

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.[156] The

---

[151] 2009 U.S. Dist. LEXIS 3051 (2009).

[152] *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 ….).

[153] *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.")

[154] *Id.*

[155] *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.")

[156] 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

misappropriation tort provides a remedy to a plaintiff where a defendant has made an unauthorized commercial use of her name or likeness.[157] There is no similar tort in Australia, even if Chang had had the wherewithal to litigate there.

Given that the issue in the *Chang* case involved unauthorized use of a photograph, one might think that the more obvious cause of action would be a copyright claim. After all, copyright law is much more harmonized globally than privacy law.[158] Australia protects copyrighted photographs to a similar extent as the United States.[159] The problem for Chang was that she was not the photographer, but rather than image subject. In most cases, the person who takes a photograph is the copyright holder with respect to that photograph.[160] The image subject is therefore hardly ever the copyright holder, unless she has contracted for the assignment of copyright, or the photograph is a work for hire.[161]

There may in fact be nothing wrong with the ultimate holding in *Chang*. 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.[162] 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.

---

privacy.")

[157] *Id.*

[158] LEAFFER, *supra* note 83, at 570 (describing the major harmonization efforts relating to copyright law at the international level).

[159] Australian Copyright Council, Photographers & Copyright, INFORMATION SHEET G011v14 (January 2006, on file with the author) ("Copyright protects a range of materials, including photographs"); LEAFFER, *supra* note 83, at 116 (noting that copyright protection for 'pictorial, graphic, and sculptural works' in the United States includes photographs under 17 U.S.C. § 102(a)(5)).

[160] Christine Haight Farley, *The Lingering Effects of Copyright's Response to the Invention of Photography*, 65 U. PITT. L. REV. 385 (2004) (tracing the history of photographic copyrights in the United States and the basis of the trend towards granting photographers copyrights in their work).

[161] 17 U.S.C. § 101 (defining "work made for hire" as: "(1) a work prepared by an employee within the scope of his or her employment; or (2) a work specially ordered or commissioned for use as a contribution to a collective work … if the parties expressly agree in a written instrument signed by them that the work shall be considered a work made for hire …..").

[162] Robertson, *supra* note 9.

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.[163] Again this is not a new phenomenon. Several pre-Internet cases were effectively resolved by a jurisdictional finding adverse to the plaintiff.[164] However, there are two reasons why Internet cases may require closer analysis with respect to jurisdiction. For one thing, 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 inquiries about developments of substantive rights. The second problem is that the substantive issues raised in Internet cases are likely to be significantly different from those raised in non-Internet cases.[165] If Internet case law disproportionately tends towards jurisdictional analysis, the development of substantive legal rights and duties online is likely to be stunted in practice.

If the cyberlaw field can contribute anything to our understanding of the law more generally, it should be able to contribute a more systematic and principled 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.

V. HARMS AND REMEDIES

---

[163] Roberton, *supra* note 9, at [2] ("In effects-test cases, the merits are inextricably intertwined with jurisdictional issues and therefore unconsciously influence the courts' decisions on personal jurisdiction.").

[164] See, for example, *ALS Scan v Digital Service Consultants*, 293 F. 3d 707 (4th Cir. 2002) (holding that maintaining a passive website that can be accessed and used by residents in the plaintiff's forum state is insufficient to support personal jurisdiction over the defendant); *Cybersell v Cybersell*, 130 F. 3d 414 (9th Cir. 1997) (holding that a passive website accessible in Arizona was insufficient to support personal jurisdiction over a non-resident defendant); *Toys R Us v Step Two*, 318 F. 3d 446 (3d Cir. 2003) (holding that the mere existence of an interactive commercial website is insufficient to establish that a defendant purposely availed itself of the plaintiff's forum state).

[165] See *supra* Part II; *infra* Part V.

A. Recognizing Online Harms

Unlike the physical world where courts will usually award damages to remedy economic harms or physical damage to a person or property, cyberspace cases will typically revolve around reputational and emotional harms. This is obvious if one thinks back to the nature of the Internet as a global communications medium. Everything that happens online happens through information exchange. There is no physical contact between people online. Thus, damages will not be physical, but psychological, emotional, or reputational.

Cyberlaw as a field needs to encompass an investigation of the kinds of online harms caused by damaging communications and, as a corollary, the appropriate remedies for those harms. For example, how does one effectively quantify the harm caused by posting an embarrassing picture or video of someone online which then goes viral and cannot be removed from the Internet once it has been shared globally? Should the law even recognize this as a harm capable of legal redress? People can be severely emotionally scarred by damaging online postings.[166] However, if there is no physical injury resulting from, say, online bullying, mobbing or harassment,[167] the victim may have been seriously wronged in a moral sense, but with no legal remedy.[168]

Professors Solove and Bartow have for some years engaged in a heated debate about whether privacy, for example, has been given short shrift by lawmakers in the digital age because there are "not enough dead bodies".[169] Solove has advocated a conception of privacy that attracts legal sanctions.[170] Bartow has suggested that perhaps the reason that legislators

---

[166] DANIEL SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET, 35-48 (2007) (giving multiple examples of people whose reputations and livelihoods were seriously injured by online gossip) [hereinafter, THE FUTURE OF REPUTATION].

[167] Jacqueline Lipton, *Combating Cyber-Victimization*, *supra* note 99, at ___ (describing examples of online bullying, mobbing and harassment).

[168] SOLOVE, THE FUTURE OF REPUTATION, *supra* note 166, at 123 ("Under our current legal system, we have remedies for defamation and invasion of privacy, but … these remedies are currently quite limited in their effectiveness, especially the law of privacy. The current law is too limited and restricted to serve as a tenable threat in many situations.")

[169] Ann Bartow, *"Nothing to Hide" Indeed: Of "Debunking" and Willful Distortions*, Madisonian.Net, May 26, 2011 (available at http://madisonian.net/2011/05/26/of-debunking-and-willful-distortions/, last viewed on August 3, 2011) (debate between Professor Bartow and Professor Solove on a popular intellectual property blog).

[170] SOLOVE, THE FUTURE OF REPUTATION, *supra* note 166, at 123-124 (describing a

and courts have not been prepared to redress some of the wrongs identified by Solove is that the harms he has identified are not yet perceived as sufficiently visceral.[171]

The point for cyberlaw studies is that many of the harms which that seemed trivial and hardly worthy of remedial action in the physical world may now merit legal redress. Whereas an embarrassing photograph or comment about an individual shared in physical space will likely only have a minor and temporary effect on that person, even a relatively innocuous photograph that goes viral online may dog the image subject for the rest of her life.[172] Internet communications require a reconsideration of the nature of harm that merits legal redress. Cyberlaw is the appropriate field within which to engage in those debates.

B. Online Wrongs Resulting in Physical Harm

Of course, in some cases, online communications can result in actual physical harm. Some of this harm can be devastating, as in the case where an individual posted an ad on Craigslist that a young woman wanted to be sexually attacked and giving her address.[173] This resulted in the woman being attacked by a person who responded to the ad.[174] Some cases of online bullying or harassment have also led to suicides of the subjects of the harmful online commentary.[175] The respective suicides of Megan Meier and

---

conception of legal remedies for online privacy invasions and other reputational damage).

[171] Ann Bartow, *A Feeling of Unease About Privacy Law*, 11 PENNUMBRA (2006), available at http://www.pennumbra.com/responses/11-2006/Bartow.pdf, last viewed on August 3, 2011 ("To phrase it colloquially, in this author's view, the Solove taxonomy of privacy suffers from too much doctrine, and not enough dead bodies. It frames privacy harms in dry, analytical terms that fail to sufficiently identify and animate the compelling ways that privacy violations can negatively impact the lives of living, breathing human beings beyond simply provoking feelings of unease.")

[172] SOLOVE, THE FUTURE OF REPUTATION, *supra* note 166, at 4 ("As social-reputation shaping practices such as gossip and shaming migrate to the Internet, they are being transformed in significant ways. Information that was once scattered, forgettable, and localized is becoming permanent and searchable."); Jacqueline Lipton, *"We, the Paparazzi", supra* note 129, at 983 ("…even if current Internet users' apparent carelessness about personal information online is temporary, the effects of this carelessness may be widespread, permanent, and devastating because of the global and increasingly archival nature of today's online content. Coupled with the aggregation and decontextualization problems …, the 'blip' of unfortunate behavior today may have serious long-term consequences for many people.")

[173] Jacqueline Lipton, *Combating Cyber-Victimization*, *supra* note 99, at ___ .

[174] *Id.*

[175] *Id.*, at ___ (describing suicide of thirteen year old Megan Meier as a result of online bullying).

Roger Clementi are tragic cases in point.[176]

In cases where online communications cause real physical harm, it is very difficult for law and policy makers to determine legal liability. Which parties in the causal chain, if any, should ultimately be held responsible? One may think that the most obvious place to start in attaching legal liability is with the person who causes the actual physical damage. However, this will not always be effective in practice. In the case of a suicide, for example, there is no physical attacker. The victim kills herself as a result of online comments.

Further, in the case of many physical assaults, the physical perpetrator of the harm may have been misled and may not have intended to cause any real damage. In the case of a fraudulent rape fantasy notice like the one posted on Craigslist, for example, the perpetrator of the physical attack may think the victim's protests are all just part of the act. In strict liability torts and crimes, the intention of the physical attacker may be irrelevant. However, in cases where the state of mind of the defendant is relevant, this may significantly diminish remedies available to the victim with respect to the activities of the physical actor.

Other than the physical actor, might liability attach to anyone else? In cyberspace-related cases, the question arises as to whether the online actors who incited the physical harm should share any of the blame for the resulting harm. The suicide of thirteen year old Megan Meier is an example of a devastating result in the physical world of morally reprehensible online conduct. One of Meier's classmate's mothers, Lori Drew, created a false persona online – Josh Evans – to start a virtual relationship with Meier in order to find out if Meier would say anything negative about Drew's daughter.[177] Ultimately, Drew used the Evans persona to torture and humiliate Meier, ultimately saying that the world would be a better place without her.[178]

As a result of Drew's hurtful words in the guise of Evans, Meier committed suicide. While Drew's actions were clearly morally wrongful, particularly as she was aware that Meier suffered from depression,[179] there was no clear basis of legal liability under which Drew could be held

---

[176] See following discussion.
[177] Jacqueline Lipton, *Combating Cyber-Victimization*, *supra* note 99, at ___.
[178] *Id*., at ___.
[179] *Id*., at ___.

responsible.[180] Federal prosecutors ultimately hinged their case on a fairly tortuous interpretation of the Computer Fraud and Abuse Act.[181] This legislation was enacted in the early days of the personal computer revolution to criminalize computer hacking– described in the legislation in terms of exceeding authorized access to a computer system.[182]

In an attempt to apply the legislation to Drew's actions, prosecutors argued that Drew had exceeded her authorized access to the MySpace computer system in creating the fake Josh Evans persona because MySpace's terms of service prohibited false identities.[183] The prosecutors' interpretation of the legislation failed because the judge was concerned that such a reading of the statute would render it void for vagueness.[184] In the court's view, it would be too difficult for anyone to be expected to know all the terms of service of the various online platforms to which they subscribed, sufficiently to avoid serious criminal liability.[185]

In the case of the suicide of eighteen year old Tyler Clementi in New Jersey, courts will be faced with arguments in favor of novel applications of state hate crimes laws in order to hold Clementi's roommate and another student criminally responsible for Clementi's death.[186] Clementi's

---

[180] *Id*., at ___.

[181] 18 U.S.C. §§ 1030(a)(2)(C) & 1030(c)(2)(A) (relating to accessing a computer system without authorization or in excess of authorization); *United States v Drew*, 259 F.R.D. 449 (2009).

[182] 18 U.S.C. §§ 1030(a)(2)(C) & 1030(c)(2)(A).

[183] Andrew M Henderson, *High-Tech Words Do Hurt: A Modern Makeover Expands Missouri's Harassment Law to Include Electronic Communications*, 74 MO. L REV 379, 393 (2009).

[184] *United States v Drew*, 259 F.R.D. 449, 464 (2009) ("The pivotal issue herein is whether basing a CFAA misdemeanor violation as per 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A) upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine. This Court concludes that it does primarily because of the absence of minimal guidelines to govern law enforcement, but also because of actual notice deficiencies. ….[T]erms of service which are incorporated into a browsewrap or clickwrap agreement can, like any other type of contract, define the limits of authorized access as to a website and its concomitant computer/server(s). However, the question is whether individuals of 'common intelligence' are on notice that a breach of a terms of service contract can become a crime under the CFAA. Arguably, they are not.").

[185] *Id*., at 467 ("In sum, if any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that section 1030(a)(2)(C) becomes a law that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet].'")

[186] John Culhane, *More than the Victims: A Population-Based, Public Health Approach to Bullying of LGBT Youth*, 38 RUTGERS L. REC. 1 (describing the limitations of current legislation in addressing bullying in situations like that involving Clementi's

roommate and the other student outed Clementi online by recording homosexual encounters involving Clementi in his dorm room and posting them online.[187]

Courts and legislators are now faced with issues of how to attach blame to moral wrongs committed online that lead to grave physical harm in the real world. There is currently great uncertainty as to which existing laws might apply to these kinds of situations and, indeed, whether any current laws are appropriately applied. It is likely that new tort and criminal laws will need to be developed to tackle these challenges in the future.[188] The cyberlaw field is a good place to initiate inquiries about how to fit these online wrongs into the legal matrix, and to develop substantive torts and crimes that fit the moral wrongs currently ocurring online.

C. Quantifying Damage

Another challenge for cyberlaw in cases where novel kinds of harms occur online is the problem of quantifying damages or ascertaining other effective remedies. Many standard legal remedies – such as damages and injunctions - do not work particularly well online. Injunctions are not effective because it is impossible to meaningfully remove harmful information from the Internet. There is a disturbingly permanent quality to online information.[189] An order to remove information from one website, or even from multiple websites, will not result in the removal of the information from the Internet entirely. Additionally, it is difficult to quantify a damages order that can make a plaintiff whole where that plaintiff is likely to suffer consequences of the online damage for the rest of her life due to the permanent and global quality of online information.

Of course, one might argue that society will eventually stop taking notice of online information, particularly information from an individual's

---

Suicide).

[187] *Id.*, at para. 2 ("Tyler Clementi is dead because the internet dissemination of videos showing him in an intimate setting with another man was too much for him to bear. He jumped off the George Washington Bridge.")

[188] Lipton, *Combating Cyber-Victimization*, *supra* note 99, at ___ (advocating legal reform alongside developments in other regulatory mechanisms such as social norms and market forces to protect individuals from online bullying and harassment).

[189] Lipton, *"We, the Paparazzi"*, *supra* note 129, at 977 (describing the impossibility of removing all iterations of a given image from the Internet); SOLOVE, THE FUTURE OF REPUTATION, *supra* note 166, at 4 ("Information that was once scattered, forgettable, and localized is becoming permanent and searchable.")

distant past.[190] The argument runs that because eventually everyone will have something embarrassing online, it will become the norm to expect this kind of information and to ignore it.[191] One may also argue that an aggrieved person should be responsible for pro-actively making access to damaging information more difficult even if it cannot be completely eradicated from the Internet. For example, the victim could utilize a service like Reputation.com to help sanitize her online reputation.[192] Assuming that society becomes more blasé about online reputation and that individuals can act to protect their own online reputations, there may ultimately be no role for the law in this context.

That may be true for the future. However, at the present time people are losing jobs and suffering reputational and emotional damage as a result of morally questionable online postings.[193] Today's law should play a role in protecting those damaged by harmful online communications. Current caseloads demonstrate that private individuals are relying on the law to vindicate their personal reputations and emotional well being. The recent *AutoAdmit* litigation in the United States is a case in point.[194] In this case, two female law students refused to stand by while they were embarrassed, defamed, and humiliated on a bulletin board.[195] The British case involving

---

[190] SOLOVE, THE FUTURE OF REPUTATION, *supra* note 166, at 49 ("perhaps generations in the future will no longer expect much privacy. One might envision a future where we can finally be uninhibited and honest about ourselves. When everybody's wants are exposed, maybe people will stop readily condemning others, and the social norms that people enforce yet secretly transgress will gradually fade away.").

[191] *Id.*

[192] See Reputation.Com, *Reputation.Com Helps Businesses and Consumers Control Their Online Lives* ("The growth of the Internet has made managing your online reputation online a necessity. Through proprietary technology we allow customers to monitor the web, delete their personal information, and control how they look when searched online.), available at: http://www.reputation.com/company, last viewed on August 3, 2011; see also MICHAEL FERTIK and DAVID THOMPSON, WILD WEST 2.0: HOW TO PROTECT AND RESTORE YOUR ONLINE REPUTATION ON THE UNTAMED SOCIAL FRONTIER (2010) (describing ways in which an individual or business can monitor and control his or her online reputation either with or without the help of a service such as reputation.com).

[193] SOLOVE, THE FUTURE OF REPUTATION, *supra* note 166, at 38 ("Employers are looking at social network site profiles of prospective employees. Microsoft officials admit to trolling the Internet for anything they can find out about people they are considering for positions. After a promising interview with a college student for a summer internship position, a company president checked the student's Facebook profile. The student listed his interests as 'smokin' blunts' and having a lot of sex. He didn't get the job …. Some big corporations are using software to systematically monitor employee blogs.")

[194] *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).

[195] *Id.*

Max Mosley, the wealthy Formula One magnate, is another example of a plaintiff suing for reputational and emotional damage caused by online and offline breaches of his privacy.[196] The *Mosley* case in particular involved a detailed examination of the problem of *quantifying* damages in the case of emotional and reputational harm outside of the more common defamation context.[197]

It is not the aim of this article to resolve issues of how to quantify and remedy online harms. The aim is rather to demonstrate the necessity of accepting and reconceptualizing cyberlaw as a field within which these kinds of issues can be debated. By understanding the nature of the Internet as focusing on global intermediated information exchanges, one can begin to better understand the challenges inherent in developing legal principles appropriate to the online world. The manner in which people communicate online, the global extent of those communications, their permanent quality, and the specific types of harms that may result are all bound up with the nature of cyberspace itself. We need a clear theoretical framework within which to study these unique aspects of the Internet in order to develop appropriate rules for identifying and remedying online wrongs. Cyberlaw is the appropriate forum for these debates.

VI. CONCLUSIONS

This article contends that cyberlaw is not, and arguably never should have been, dismissed as a "law of the horse". While it was unclear in the early days of the Internet how the field would develop in terms of substance, it is much clearer now that cyberlaw is, and should remain, a distinct field. The benefits of recognizing and developing cyberlaw as a field derive from the fact that there are aspects of the Internet that create unique legal challenges. The Internet is, above all else, a tool for global communications. All Internet interactions are information exchanges, and all of those exchanges are enabled by one or more intermediaries. Most of these exchanges have a permanent and global quality that can ultimately result in significant personal and reputational harms.

A field of cyberlaw will comprise legal issues that arise out of the unique nature of the Internet. It will include a detailed consideration of the legal responsibilities of Internet intermediaries of all kinds and in many

---

[196] *Mosley v. News Group Newspapers Ltd*, [2008] EWHC (QB) 1777, [2008] E.M.L.R. 20 (Eng.).

[197] *Id*., at para 212-231 (describing difficulties of quantifying damages in privacy infringement cases involving emotional and reputational harm).

contexts. However, it must also incorporate jurisdictional considerations, the relationship between legal rules and online norms, the identification of remediable online harms, and the ability to develop effective and apropriate remedies for those harms. The cyberlaw field will overlap with other more traditional bodies of law such as tort, contract, criminal law, constitutional law, and intellectual property law. However, a consideration of problems common to the Internet within the cyberlaw field will lead to more principled, systematic and effective legal developments.

While debates about the nature of cyberspace and about the ability of national governments effectively to regulate cyberspace have continued since the dawn of the Internet, the debate about the nature of cyberlaw as a field has stalled. It is now time to revive this debate. The Web 2.0 era has broadened the reach of the Internet by enhancing how, and how often, we interact online. We are no longer relatively passive consumers of online information. Rather, we increasingly participate in creation and dissemination of content, often causing harm to others in the process. As more and more people interact with each other online at an exponential rate, it is imperative that a cyberlaw field can be developed and organized in a way that reflects the realities of the Web 2.0 generation. Whatever the nature of cyberlaw in the past, it is now time for a Cyberlaw 2.0.