K. A. Taipale
February 2003 v.1.01C • CAS Working Paper Series No. 04-2003
http://www.advancedstudies.org/papers/SecLia.pdf

Secondary Liability on the Internet: Towards a Performative Standard for Constitutive Responsibility.

"The data has passed out of the physical plane and into the mathematical, a higher and purer universe where different laws apply." [FN 1]

"The Internet is a unique and wholly new medium of worldwide human communication." [FN 2]

PRELUDE

New technologies provide new opportunities and new potentials. Although the Internet has the potential to be a great liberating forum for human expression, it also has the potential to be an abyss of human avarice filled with pornography, defamatory statements, stolen intellectual property, destructive viruses, intrusive spam, and other harmful things.

The question is no longer should the Internet be regulated but how. [FN 3] In this debate, one side asserts that "cyberspace" [FN 4] is a "unique and wholly new" thing – so different as to

---

1 Neal Stephenson, on the first "Turing" computer of the 1940s, "Cryptonomicon," (1999), cited in Stuart Bigel, "Beyond Our Control: Confronting the Limits of Our Legal System in the Age of Cyberspace," Cambridge: MIT Press (2001) at p. ix.

2 Reno v. ACLU, 521 U.S. 844, 850 (1996).

3 Among certain segments of early Internet pioneers (the "cyber-libertarians") there was (and still is to some degree) an unrealistic expectation that the Internet was beyond any regulation. For a metaphorically excessive expression of this view, see John Perry Barlow, the self-deluded "Thomas Jefferson of Cyberspace", co-founder of the EFF, and ex-lyricist for the Grateful Dead, who declared in 1996:

> "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. … Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here."

"A Declaration of the Independence of Cyberspace" at http://www.eff.org/~barlow/Declaration-Final.html.

Of course, in reality, the Internet was always subject to regulation. First through social norms, see generally Rob. C. Ellickson, "Order Without Law," Cambridge: Harvard University Press (1991) and Lawrence Lessig, "The Regulation of Social Meaning," 62 U. Chicago L. Rev. 943 (1995), and, second, through code, see "Code is Law," pp. 3-8 in Lawrence Lessig, "Code and other Laws of Cyberspace," New York: Basic Books (1999). Thus, the question was never 'should' cyberspace be

require new laws or doctrine, maybe even its own transnational jurisprudence. [FN 5] The other side decries that while the technology is new the legal problems are familiar and existing legal doctrine and analysis can easily accommodate the new developments. [FN 6] As with all such debates, neither side is entirely correct.

Determining where old doctrines can be extended to new circumstance or where new doctrines are required to fill interstitial gaps in old theory requires understanding how, and to what extent, the process of digital mediation itself affects the theoretical foundations that have provided the basis for accepted legal practice in the physical world ("realspace").

Because cyberspace is fundamentally a medium of human communication, its regulation implicates important core principles of democratic governance [FN 7] – including the ownership of intellectual property, and the rights to privacy and free expression – each with its own doctrinal schema. [FN 8] Ascription of legal responsibility for online behavior involves balancing social harms with individual freedoms within a complex constitutional and technological framework.

---

regulated but rather 'by whom' – now that it is clear that existing "governments" will have a role, the question is 'how'. See also the discussion of "Coercive Power", infra Part I.

4 We use "cyberspace" to mean the electronic medium of computer networks, in which online communications takes place, the system of interconnected "switches and pipes" that comprise the digital, packet based communications network. See Reno v. ACLU, 521 U.S. 844, 851 (1997):

> "All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium—known to its users as "cyberspace"—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet."

The term "cyberspace" is credited to William Gibson, "Neuromancer", New York: Ace Books, Reissue edition (1995, 1984) p. 51:

> "Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts … . A graphical representation of data abstracted from the banks of every computer in the human system."

5 See, for example, David R. Johnson and David Post, "Law and Borders: The Rise of Law in Cyberspace," 48 Stanford L. Rev. 1357 (1996) (stating the case for cyberspace sovereignty). See generally Llewellyn J. Gibbons, "No Regulation, Government Regulation, or Self-regulation: Social Enforcement or Social Contracting for Governance in Cyberspace," 6 Cornell J. Law and Public Policy 475 (1997).

6 See, for example, Jack L. Goldsmith, "Against Cyberanarchy," 65 U. Chicago L. Rev. 1199 (1998) and Christopher M. Kelly, "The Cyberspace Separatism Fallacy: BOOK REVIEW: Curtis Karnow, Future Codes: Essays in Advanced Computer Technology and the Law," 34 Texas Int'l. L. J. 413 (1999). And see Lawrence Lessig, "The Zones of Cyberspace," 48 Stanford L. Rev.. 1403, 1407-1410 (1996) (criticizing Johnson and Post, supra footnote 5).

7 See Reno v. ACLU, 521 U.S. 844, 850 (1996).

8 In this regard, see Timothy Wu, "Application-Centered Internet Analysis," 85 Virginia L. Rev. 1163,1170-1172 (1999) in which he criticizes Reno v. ACLU, supra, for "group[ing] in one constitutional box a huge range of highly variable Internet usage" and arguing for an application centered approach.

While we wholly agree with Wu's analysis, this paper is concerned with articulating various over-arching theoretical construct useful for analyzing online behavior. Obviously, the application of any of these constructs is wholly dependent on the contextual setting and thus the particular service or computer application under review, for example, email versus web publishing. Therefore, we only draw such distinctions in this paper to the extent that they are required to illustrate aspects of the theoretical principles.

Reconciling these disparate doctrines is further complicated in discussions of secondary liability – the doctrine under which a third party is held responsible for the misconduct of another – because the standard legal analysis usually confines itself to the particular doctrinal issue at stake rather than with articulating an overarching theory for imposing such third party liability. [FN 9]

This paper examines certain theoretical constructs in law, legal theory and communication that relate to secondary liability and its applicability to regulating online behavior.

The central thesis of this paper is that a theoretical basis for ascribing legal responsibility to third parties can be based on that party's constitutive role in enabling illegal acts of others to produce social harm. Specifically, that the provision by an Internet service provider (ISP) of access to the enabling technical infrastructure – the network medium – in itself creates a responsibility base for mitigating social harm arising from the use of that infrastructure based on the effects of the mediation in furthering or contributing to the harm. [FN 10]

INTRODUCTION

Technological developments do not determine human fates; rather, they change the spectrum of opportunities and potentials within which people act. [FN 11] The global reach of the Internet, the ease and low marginal cost of replication and transmission of digital data, and the relative anonymity of users have changed the balance of forces that have previously served to keep in check certain undesirable behavior in the physical world.

These characteristics of cyberspace have lowered the cost of perpetrating undesirable behavior by eliminating certain barriers to entry and by lowering transaction costs of committing cyberwrongs. [FN 12]

At the same time, however, other characteristics of cyberspace provide new opportunities to control illegal acts. Unlike the physical world, in cyberspace certain readily identifiable third parties – Internet service providers ("ISPs") [FN 13] – have exclusive technical control over user

---

9 Thus, for example, the different standards for third party liability in cases of defamation, copyright infringement, securities fraud, sexual harassment, etc. Some of these standards are discussed in greater detail in Part II, infra.

10 See discussion in Part I, infra.

11 Robert McClintock and K. A. Taipale, "Educating America for the 21st Century," Circulation Draft, Version 2.1, September 1994, New York: Institute for Learning Technologies, Columbia University, available online at http://www.taipale.com/ilt/ILTplan.html .

12 Neal Kumar Katyal, "Criminal Law in Cyberspace," 149 U. Penn. L. Rev. 1003, 1006 (2001).

13 ISPs provide a variety of network related services, for example, network access, hosting services or online content services. For our purposes, unless otherwise stated, we use ISP to include all types of services. For a statutory definition of "service provider", see 17 U.S.C. §512(k) and see ALS Scan v. RemarQ Communities, 239 F.3rd 619, 623 (4th Cir. 2001) (the DMCA "defines service provider broadly").

However, note the discussion of scalarity, infra in Part I, and the implications of providing a particular service to the ascription of third party responsibility for its use. And, see Wu, supra footnote 8.

misconduct because they control access to the network. Unlike users, these ISP gatekeepers are easily located and thus easily available for legal sanction.

It should be noted that the general notion of imposing liability on ISPs for the misconduct of their users is accepted as a "given, and … is justified due to the ability of the Internet service providers to prevent subscriber misconduct cheaply." [FN 14] The controversy, to the extent that there is one, is to determine the scope and standards for assigning such liability to ISPs without creating other inefficiencies, for example, overdeterrence of desirable or protected behaviors. [FN 15]

The purpose of this paper is to explore certain theoretical constructs in order to develop an analytic framework that is potentially useful in delineating the appropriate scope, and under what circumstances and rationale, legal responsibility can be ascribed to ISPs for the actions of their users. [FN 16]

Thus, in Part I we examine the theoretical basis for legal responsibility; in Part II, we review the existing doctrines of secondary liability as applied in particular contexts, (copyright, defamation, *respondeat superior*) [FN 17]; in Part III, we suggest a performative standard for assessing ISP liability; in Part IV, we develop a preliminary approach for applying a constitutive standard for third party liability to ISPs; and, in Part V, we set out areas for further development.

This paper should be considered a preliminary research agenda rather than as a definitive statement on these issues.

---

14 Assaf Hamdani, "Who's Liable for Cyberwrongs?" 87 Cornell L. Rev. 901, 911 (2002) ("following doctrine and academic literature, this Article takes ISP liability as a given … ").

15 Ibid. "[T]here is a controversy over identifying the standard that should govern ISP liability for user misconduct. This aspect of third-party liability, which has remained curiously unexplored in the economic literature, is the focus of this Article." Hamdani's article examines in some detail the deterrence effect of ISP liability from a social utilitarian and economic theory perspective. Hamdani argues that imposing strict liability on ISPs results in the adoption of "excessive levels of monitoring and employ[ment of] overly zealous censorship policies" (p. 905) because ISPs do not capture the full value of the user's conduct. That is, holding ISPs strictly liable for the full social harm of user conduct where they do not gain the full value from the conduct, creates an incentive structure that leads to over-regulation.

16 It should be noted that the conceptual basis set forth in this paper for analyzing ISP liability is applicable in other areas where a third party has technical control over the behavior of others or over the reach of such behavior. Thus, the same theoretical approach can be applied to hyperlinking, and, although more doctrinally problematic, to ascribe affirmative duties on network service providers such as search engines and other utility providers. This latter point is discussed briefly in footnote 48 infra and its accompanying text.

17 Although we confine our review mostly to copyright, defamation and employer liability under the doctrine of *respondeat superior*, the same analysis presented here would apply to other substantive areas of the law, including, for example, obscenity and hate speech, as well as harmful software such as viruses, worms and other malicious code.

PART I. Legal Responsibility (and Coercive Power) in a Postmodern World.

This section examines the concepts of constitutive responsibility and, briefly, coercive power, and their theoretical relationship to third party ISP liability.

Constitutive Responsibility

In "Harmful Thoughts: Essays on Law, Self and Morality," Meir Dan-Cohen sets out a theory of responsibility based on what he calls the "constitutive paradigm". [FN 18]

Traditional notions of legal responsibility based on blame – that is, ascribing moral responsibility for the consequences of one's actions – are premised on what is generally known as the "free will paradigm". In the free will paradigm, responsibility is ascribed to an actor based on their capacity to choose their actions freely. [FN 19]

"Whereas the free will paradigm treats responsibility as a matter of what we choose to do, the constitutive paradigm treats responsibility as a matter of what and who we are." [FN 20] That is, constitutive responsibility is a function of one's social 'role' in relation to a given action or conduct.

Dan-Cohen's analysis is presented from the viewpoint of the self and he explores the concept of responsibility in terms of where, for legal purposes, responsibility intersects with the "boundaries of the self." [FN 21] However, his pertinent insight for our purposes is to outline the dual structure of responsibility and to distinguish between "object-responsibility" and "subject-responsibility". [FN 22] Object-responsibility relates to direct authorship of an event or behavior while subject-responsibility relates to the responsibility base for which object-responsibility may be assigned.

To illustrate, in the context of an accident brought on by drunk driving, the driver can be ascribed object-responsibility for the accident and/or subject-responsibility for the condition that resulted in the accident, i.e., drunk driving. Drunk driving is the responsibility base for attributing object-responsibility for the accident.

> "In short, my suggestion is that the structure of responsibility and its meaning are to be found in a relationship of mutual implication between object- and subject-responsibility. The ascription of object responsibility implies a certain responsibility base and hence a certain subject-responsibility. Conversely, the ascription of subject-responsibility designates a responsibility base and hence range of object-responsibility for objects and events that emanate from that base." [FN 23]

---

18 Meir Dan-Cohen, "Harmful Thoughts: Essays on Law, Self and Morality," Princeton: Princeton University Press (2002) at199-241.

19 Ibid. at 199-200.

20 Ibid. at 201.

21 See generally "Chapter 7: Responsibility and the Boundaries of the Self," in Dan-Cohen, supra footnote 18, at 199-245.

22 Ibid. at 202-204.

23 Ibid. at 203.

Dan-Cohen goes on to examine how the individual and social conceptions of the self are implicated under this approach to responsibility. It is beyond the scope of this paper to fully summarize Dan-Cohen's analysis here, but the salient points for our purposes include the concept of modularity – that is, the correspondence between the socially accepted conception of the self and the particular manifestations of self – and the concept of scalarity – that is, the fluidity between role and responsibility depending on the context and its relationship to a central or peripheral element of self conception. [FN 24]

It is our intention to apply these concepts to third party ISP liability. [FN 25] Thus, in our analysis, modularity refers to the correspondence between the assumption of a role (that is, the service provided as a business matter) with the social expectations ascribed to that role (that is, the responsibility for subsequent harm resulting from the use of such services). [FN 26] And, scalarity, for our purposes, refers to the relationship ("closeness") of the service provided (that is, the service that enables the illegal act) to the core of the role of the ISP. [FN 27]

---

24 Ibid. at 209-215.

25 Of course, these concepts can be applied to third party liability in the physical world. For instance, in our earlier drunk-driving example, third party liability might be extended to the person who supplied the alcohol to the driver.

Analysis of modularity would be concerned with the relationship between the third parties assumed role and their ascribed role. (For instance, did they assume the role of "friend" but society ascribes them the role "bartender" or "host" with attendant responsibility).

Analysis of scalarity would concern itself with how central the supplying of alcohol was in this particular case to the role of the third party. (For example, distinguishing the centrality to the third party role between a beer stolen from a friend's refrigerator and a triple martini served to an intoxicated patron in a bar as part of 'happy hour'.)

The third party might then be ascribed subject-responsibility (a responsibility base for the drunkenness of another) by virtue of their role (i.e. bartender or host) with object-responsibility for the drunken state of the driver (which, in turn, is a responsibility base for the accident itself). It is obvious from this example that the interplay between object-responsibility and subject-responsibility is implicit in traditional legal formulations of "causation".

26 For example, modularity in this sense refers to the relationship between providing a "staple of commerce" and its subsequent illegal use. See generally the discussion in Sony v. Universal Studios, 464 U.S. 417, 439-442 (1984).

27 That is, the particular service and its relationship to the harmful conduct. In the case of ISPs this includes the distinction that underlies arguments about whether "access" or "hosting" services give rise to different levels of responsibilities.

For example, the applicability of the DMCA 15 U.S.C. §512(h) subpoena provisions to an access provider was at issue in RIAA v. Verizon (DCDC 02-MS-0323-JDB, decided January 21, 2003). Verizon's position was that because it was not offering hosting services (the illegal material was not stored on its system) it should not be subject to the provision of §512(h).

Although the court's decision in Verizon turns on narrow grounds of statutory interpretation, the court's discussion of policy, Verizon at 18, does reflect the scalarity of access to the service provided. It is access to the network that gives rise to the harm, and it is this network availability that is the functional role of the ISP that Congress was addressing. Thus, to artificially circumscribe "storage" or "hosting" as the subject of §512(h) procedures would frustrate the purpose of the statute:

> "Verizon has provided no sound reason why Congress would enable a copyright owner to obtain identifying information from a service provider storing the infringing material on its system, but would not enable a copyright owner to obtain identifying information from a service provider transmitting the material over its system … ." Verizon at 18.

In addition to ascribing responsibility based on volition and character traits, Dan-Cohen examines three other dimensions along which the "self can be constituted: the spatial, the temporal, and the social." [FN 28] We examine how each of these dimensions is implicated in secondary liability.

First, the spatial refers to responsibility for the body and property (other objects) and refers to strict responsibility, that is, responsibility for the consequences of one's bodily actions or actions involving one's property. Note that under this analysis, Dan-Cohen includes vicarious liability as a direct extension of the self. [FN 29]

Traditional notions of vicarious liability are based on this notion of body and property. [FN 30] For example, parental or agent/employee responsibility arises because control is considered to be an extension of the self. Here the act of a subordinated other is considered an act of the superior "self", that is, an extension of the superior "body or property". [FN 31]

Second, the temporal dimension refers to the responsibility for the actual results of the conduct. Here the constitutive paradigm accommodates, for example, the difference in punishment between an attempted murder that is unsuccessful due to unforeseen intervening events and the successful murder. [FN 32] Although the conduct was the same, the difference in punishment can be understood in relationship to the difference in actual outcome by viewing such outcome as "an ineluctable fact within [the] boundaries that constitute [the responsible party's] identity as a murderer." [FN 33].

Under our analysis in the context of ISP liability, proportional responsibility may then attach for the effect that the provision of a particular service gives to the illegal behavior. The service role of the ISP itself encompasses the actual result of the use of that service by another to engage in illegal conduct. To put it another way, the illegal conduct is a fact within the boundaries that constitute the ISP's identity (the "corporate self" defined by its services). [FN 34]

For example, the amplification effect of certain services on the network gives behavior different potential harm effects and may therefore implicate different levels of responsibility by including the consequential result within the defined service. [FN 35] Even "access only" service has variable harm effects depending on the technical characteristics or conditions of the service

---

28 Dan-Cohen, supra footnote 18, at215.

29 Ibid. at 218.

30 Vicarious liability is discussed below in Part II. The spatial extension of self is implicit in the traditional legal formulation of "control".

31 The responsibility base arises by virtue of the presumed control over subordinate actors.

32 Dan-Cohen, supra footnote 18, at 219-221.

33 Ibid. at 221. The responsible party is viewed as subject-responsible for the consequence of being a murderer, rather than just object-responsible for the conduct resulting in death.

34 See A&M Records v. Napster, 114 F. Supp.2d 896, 917 (N.D. Ca. 2000) (focusing on "Napster's primary role of facilitating the unauthorized copying and distribution … ") Although Napster was not providing a traditional ISP service, see supra footnote 13, our analysis is applicable to the provider of any online service that "exercises ongoing control over its service," Napster at 916, where such ongoing control puts the resulting harm within the 'boundaries' of the service provided, i.e., the ISP's identity.

35 See also Wu, supra footnote 8 (arguing for an application-centered approach to regulating cyberspace).

provided. [FN 36] We might say that network access is object-responsible for harm, but the conditions of access are subject-responsible for harmful effect. [FN 37]

Finally, the social dimension refers to collective responsibility. Under the Western notion of jurisprudence, accustomed as it is to an individual moral ontology, collective responsibility is generally only assigned under two narrowly circumscribed and contrary approaches.

Either the collective itself (that is, the group as a fictional "self") is thought to directly author the event (thus, the corporation or union is held responsible) or we ignore the group and hold that group action is always reducible to the action of individuals. [FN 38] By ascribing collective responsibility, we either hold the group itself responsible for the action of its individual members or we implicitly hold some individuals responsible for the actions of others. [FN 39]

Dan-Cohen presents another view of collective responsibility based on his conception of constitutive responsibility. Here subjects of collective responsibility are individuals whose responsibility is primary and direct, rather than secondary and vicarious, by virtue of their social identity being a legitimate "constituent of the self that can serve as an individual responsibility base for the group's collective endeavors." [FN 40] In other words, responsibility accrues because of the social role or membership in a group. [FN 41]

---

36 For example, the total amount of bandwidth provided, the symmetry of up and downstream bandwidth, the addressing scheme (dynamic versus static IP address), and firewall filtering and access port enabling or disabling all have significant effect on both whether illegal acts can occur in the first place and on the severity (social cost) of their harm if they do.

The temporal dimension of responsible self is implicit in traditional legal formulations of "foreseeability".

37 Both modularity and scalarity are implicated as well – modularity in ascertaining the correspondence between the ISPs role and its legally defined responsibilities (for example, telephone versus broadcast versus cable), and scalarity in ascertaining how central the responsibility base is to the ISP's role or the harm being addressed.

In a sense, this entire approach is merely another way of stating that the law should develop more sophisticated analytical tools than the purely categorical.

38 Dan-Cohen, supra footnote 18, at 222. And see Joel Feinberg, "Collective Responsibility," in "Doing and Deserving," Princeton: Princeton University Press (1970) at 233. See also, Eli Lederman, "Models for Imposing Corporate Criminal Liability: From Adaptation and Imitation toward Aggregation and the Search for Self-Identity," 4 Buffalo Criminal L. Rev. 641 (2000).

39 An example of the latter is the felony-murder rule, in which a participant in the underlying felony is held responsible for a murder committed by an accomplice in such felony. For a discussion of whether such liability is premised on a theory of agency or proximate cause, see Jennifer DeCook Hatchett, "Kansas Felony Murder: Agency or Proximate Causation," 48 Kansas L. Rev. 1047 (2000).

Another example is criminal conspiracy, in which each co-conspirator can be held criminally liable for the acts of the others. See generally, Raphael Prober and Jill Randall, "Federal Criminal Conspiracy," 39 American Criminal L. Rev. 571 (2002).

40 Dan-Cohen, supra footnote 18, at 222.

41 Examples of such liability are gang membership or membership in an organized crime enterprise. Note that in the United States, so-called "status crimes" are generally prohibited without an additional element of actus reas. See generally, Jocelyn L. Santo, "Note: Down on the Corner: An Analysis of Gang-Related Anti-loitering Laws," 22 Cardozo L. Rev. 269, 286-290 and 310-311 (2000). However, gang membership can be viewed as an act of ongoing criminal conspiracy. See generally the discussion of The Racketeer Influenced and Corrupt Organization Act ("RICO"), 18 U.S.C. §§1961-1968 (2000) in Artie Jones, John Satory and Tyler Mace, "Racketeer Influenced and Corrupt Organizations," 39 American Criminal L. Rev. 977 (2002).

For our purposes, the social dimension of ISP responsibility for its user's conduct can be found in the relationship between the ISP and its "user group" or the bond between its services and its user's conduct. It is participation by the ISP with the user in the social construction of the harm that inures legal responsibility.

Coercive Power

Cyber libertarian views [FN 42] that cyberspace should be largely immune from state regulation often are premised on an Austinian [FN 43] conception of state power based on an implicit formal triangle of sovereign, citizen and right. According to this view, state regulation could not extend to cyberspace because its very nature – the technology of the medium, the geographic distribution of its users and the nature of its content – would preclude the effectiveness of any attempted regulation because there is no sovereign-citizen relationship. [FN 44]

Of course, this view ignores the ways in which private power regulates online behavior unfettered by doctrinal constraints. [FN 45] Postmodern philosophical thought, particularly that of Michel Foucault [FN 46], focuses on the more subtle informal mechanisms of coercion organized around the concepts of "surveillance and discipline", rather than power-as-sovereign. [FN 47] Foucault and commentators of like mind [FN 48], use this observation to critique the existing power structure, particularly by pointing out how traditional notions of power-as-sovereign are used to conceal the actual procedures (and thus the resulting "violence") of power in society.

We seek here, instead, to appropriate this insight to further underpin ascription of legal responsibility to third party service providers. With respect to online behavior, power over individual action is exercised by ISPs through control of identity (cf. surveillance) and access (cf.

However, the salient point is not criminal liability, which may for other reasons require an additional element, but legal responsibility. Self- or social-identification with a collective group creates subject-responsibility for the conduct of other group members. Criminal liability may require an additional showing. The social dimension of responsibility is implicit in the traditional legal formulation of 'conspiracy' and 'criminal enterprise'.

42 See footnote 3 supra, in particularly Barlow, and see footnotes 5 and 6 supra.

43 John Austin, "The Province of Jurisprudence Determined," Amherst, NY: Prometheus Books (2000, 1832). Austin defined "positive law" as that decreed by a sovereign or government.

44 See James Boyle, "Tenth Annual Corporate Law Symposium: Intellectual Property Law for the Twenty-first Century: Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors," 66 U. Cin. L. Rev. 177, 183 (1997). However, compare Timothy S. Wu, "Cyberspace Sovereignty?" 10 Harvard Journal of Law and Technology 647 (1997) (arguing against the descriptive assumption that cyberspace cannot be regulated).

And see Jack L. Goldsmith, "Against Cyberanarchy," 65 U. Chicago L. Rev. 1199 (1998) (arguing that both the descriptive and normative claims of regulation skeptics are wrong, at 1200, and that existing "real world" legal conceptions can be applied to cyberspace, at 1212-1239.)

45 See footnote 3 supra, in particularly Lessig, and see footnotes 5 and 6 supra.

46 Michel Foucault, "The Archaeology of Knowledge," New York: Pantheon (1982, 1972) and Michel Foucault, "Discipline and Punish: The Birth of the Prison," New York: Vintage Books (1979).

47 See Boyle, supra footnote 42, at 186.

48 For example, Boyle, supra footnote 42.

discipline). Users are subject to control through such power as a result of technological and business decisions made by ISPs about their services. [FN 49]

The very existence of the power to control potentially harmful conduct by others is sufficient rationale to ascribe responsibility for its use. [FN 50] Further, where, as here, it is the provision of service itself combined with the individual action that results in the conduct having harmful effect, an affirmative duty to control behavior through such service is justified.

Part I Summary

Applying the constitutive paradigm for legal responsibility, ISPs can be ascribed liability for providing access to the network and for their user's misconduct in so far as network access (or other services) give the conduct its effect. ISPs acquire subject-responsibility by virtue of their role in enabling the condition for user misconduct and object-responsibility for the online status of their user itself. These dual responsibility relationships provide a responsibility base for the harmful affects of the user's behavior.

Additionally, the possession and exercise of the power to control harmful online conduct is itself a basis for assigning responsibility for mitigating the social harm.

---

49 As discussed in footnote 34 supra, even absent any additional service layer, technical and business decisions for 'simple access' services exert significant control over potential online behavior. Decisions regarding the amount and availability of a/symmetric bandwidth, static versus dynamic IP addressing, and port filtering or other firewall control significantly enable or constrain individual user's ability to engage in illegal activity.

50 Obviously, others argue that it is the contrapose, that absent the need to mediate between competing property rights, government has no authority to intervene in private relationships. (And, they say, since cyberspace tolerates no property rights there is no legitimacy for state intervention here.) We do not need to address those arguments in this paper. Our conclusion that the existence and exercise of sovereign-like power is sufficient to justify imposition of social responsibility on actors is not central to the analysis developed elsewhere in this paper. It is, however, among the theoretical foundations for an argument that online service providers, for example, search engines and other central utilities, might be subject to other affirmative responsibilities, such as nondiscrimination, open access, or even content regulation, under an expanded theory of "public utility" or "common resource".

This topic may be explored in a future paper. In the meantime, see SearchKing v. Google (D.C. Okl. CIV-02-1457-M, January 13, 2003) (does a search engine have a duty to maintain listing?) and "What Symantec Knew but Didn't Say" (available at http://go.hotwired.com/news/infostructure/0,1377,57676,00.html) (discussing whether the security software firm Symantec had an obligation to publicly disclose what it knew about the Slammer worm at the same time that it disclosed such information to its paying customers.)

PART II. Traditional Notions of Secondary Liability

This section briefly reviews certain existing approaches to defining third party liability [FN 51] across three doctrinal areas of the law: defamation, copyright, and employer liability under the *respondeat superior* doctrine. It is beyond the scope of this paper to explore in great detail these specific doctrinal areas. Rather, we seek to identify common characteristics that relate to concepts of responsibility and regulation that concern us here.

Defamation

Defamation involves making (i) a false and defamatory statement about a second person (victim), and (ii) the publication (communication) of that statement to a third party. [FN 52] Traditional legal doctrine provides that the classification of the defendant as either a publisher, distributor, or common carrier affects the burdens to be established.

Upon the requisite showings, a publisher [FN 53] is held strictly liable for a defamation, a distributor [FN 54] is only held liable if it is shown that they knew or had reason to know of the defamatory statement, and a common carrier [FN 55] is not held liable at all.

---

51 The term "third party" is used to distinguish third parties from primary actors and victims (second party). See footnote 8 in Hamdani, supra footnote 14.

52 See Restatement (Second) of Torts, §558 (1977). Additional elements may be required depending on the status of the victim as "public" or "private", see New York Times v. Sullivan, 376 U.S. 254 (1964), where some requisite degree of fault ("reckless disregard") may be required as to the falsity of the statement. Restatement §580A. Additionally, in some cases, proof of special harm by the publication may be required.

53 Generally, the author and any party who exercised editorial control over the material or whose business it is to disseminate the content (for example, newspapers, book publishers, broadcast stations, etc.). See Restatement, supra, §577. Note that a "republisher", that is, one who repeats or otherwise republishes defamatory material, "is subject to liability as if he originally published it." Ibid. §578.

54 Distributors are those who do not participate in the production of the material but merely assist in the distribution, for example, libraries, newsstands, bookstores, and paperboys have been held to be distributors. See Restatement, supra, §581.

55 For example, the telephone companies. See Restatement, supra, §581 (but cf. comment f). In general, however, common carrier status gives rise to certain other responsibilities, such as nondiscrimination in carriage, open access, etc. It is beyond the scope of this paper to fully explore the common carrier doctrine. For a brief discussion of common carrier immunity, see Henry H. Perritt, Jr., "Tort Liability, the First Amendment, and Equal Access to Electronic Networks," 5 Harvard J. Law and Technology 65, 92-95 (1992). However, we briefly address the underlying rationale here in order to distinguish our general approach to ISP liability.

Common carrier status for telephone service providers is appropriate for regular voice service because such carriers do not have actual control over the content without engaging in real-time monitoring and censorship. Some argue that this analysis should be applied to ISPs. In our view, however, the analogy to telephone service only holds, to the extent that it is relevant at all, to email service, which shares certain characteristics with POTS ("plain old telephone service").

However, in the context of web publishing – regardless of whether the material is hosted by the ISP or the ISP merely provides access to the network – the rationale for common carrier status does not seem to apply. Here, a doctrine akin to distributor liability seems more appropriate (or, where the ISP has the requisite involvement in the production of content, original publisher liability). See footnotes 54 and 55 infra and accompanying text. Under the distributor rationale, the ISP is not responsible for

The first Internet defamation cases applied this traditional approach. In Cubby v. CompuServe [FN 56] the court held that the Internet service provider, CompuServe, was not liable for a defamatory posting to an online newsletter because it distributed the newsletter without knowledge of the allegedly defamatory statements (applying the "distributor" classification).

However, in Stratton Oakmont v. Prodigy [FN 57], another New York court held Prodigy liable for anonymously posted online comments. The court distinguished Prodigy from CompuServe because Prodigy had held itself out as a family-oriented site that exercised editorial control over posted materials.

Under the analysis that we have developed so far, the court in Stratton Oakmont could be said to have found that Prodigy assumed subject-responsibility for the editorial role, which then served as the responsibility base for assigning object-responsibility for the defamation. In Cubby, CompuServe had not assumed such a role and the court refused to attribute such responsibility (there was no divergence in modularity).

In response to Stratton Oakmont, Congress enacted Section 230 of the Communications Decency Act of 1996 [FN 58] to essentially provide ISPs with protection for liability as a "publisher". [FN 59] The plain language of the statute as well as a straightforward reading of the legislative history make clear that Congress intended that ISPs would remain liable as distributors where it was shown that they knew or should have known of the defamatory content. [FN 60]

Particularly since Congress provided immunity for those ISPs who voluntarily and in good faith blocked or removed offensive material [FN 61] in order to encourage the kind of editorial control that resulted in liability in Stratton Oakmont.

Nevertheless, in Zeran v. America Online [FN 62] the Fourth Circuit adopted a broad, and in our view incorrect, reading of the statutory grant of immunity, holding that immunity extended to ISPs regardless of their classification as either publishers or distributors. [FN 63]

The court's erroneous interpretation of the statute negates the primary purpose of §230, which was to encourage ISPs to exercise editorial control without incurring liability under the approach

---

the original publication but the ISP's control over network access gives rise to re-publisher liability upon sufficient "knowledge" of the illegal act. See footnote 66-68 infra, and accompanying text.

56 Cubby v. CompuServe, 776 F. Supp. 135 (S.D.N.Y. 1991).

57 Stratton-Oakmont v. Prodigy, No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

58 47 U.S.C. §230 (1996)

59 The language of §230 provides: "no provider … shall be treated as the publisher … of any information provided by another information content provider." 47 U.S.C. 230(c)(1).

60 See Barry J. Waldman, "A Unified Approach to Cyber-liable: Defamation on the Internet, A Suggested Approach, 6 Richmond J. of Law and Technology 9 (1999) and Robert M. O'Neil, "The Drudge Case: A Look at Issues in Cyberspace Defamation, 73 Washington L. Rev. 623, 627-629 (1998).

61 47 U.S.C. §230(c)(2).

62 Zeran v. America Online, 129 F.3rd 327, 332-334 (4th Cir. 1997).

63 See generally Paul Ehrlich, "Cyberlaw: Communications Decency Act §230," 17 Berkeley Technology L. J. 401 (2002). And, cf. footnote 65 infra.

adopted in Stratton Oakmont. By eliminating any liability for ISPs, even as distributors with knowledge of the defamatory posting, the court has created a disincentive for ISPs both to prevent defamation as well as to mitigate harm from ongoing illegal acts even with actual knowledge and control thereover. [FN 64]

Despite Zeran, the general principles for third party liability in defamation highlight an interesting aspect to "secondary" liability, that is, in general, secondary liability in defamation is actually primary liability for third party actions that serve to either publish or re-publish the defamation. [FN 65]

Liability in defamation cases is also found where the third party has control over the instrumentality of the ongoing defamation. [FN 66] Thus, for example, a tavern owner is liable for not removing a defamatory statement from the wall of the restroom after he becomes aware of it. [FN 67] The owner is not held liable for the original publication but incurs liability for its continuation upon acquiring notice. [FN 68]

So, third party liability in defamation (absent the Zeran view of CDA §230) is based on finding a primary responsibility base for the act of publishing – either as an original publisher where there is editorial involvement, or as a re-publisher where the power to mitigate and actual knowledge give rise to an affirmative duty to prevent continuation of the harm.

---

64 Ibid. See for example Doe v. America Online, No. SC94355 (Florida Sup. Ct. March 8, 2001) (holding that AOL was not liable in a case in which they did not remove defamatory material where they had actual knowledge). See also, Blumenthal v. Drudge, 992 F.Supp. 44, 51 (DCDC 1998) in which the court expressed its frustration with the Zeran interpretation of §230 that allowed AOL to contract for and post a defamatory statement, while not facing liability for its falsity. See also, Michelle J. Kane, "Electronic Commerce: Internet Service Provider Liability: Blumenthal v. Drudge," 14 Berkeley Tech. L. J. 483 (1999).

65 See Restatement (Torts) §578. Indeed, even distributor liability can be viewed as primary liability. Under such an analysis, the distributor is considered to be a "publisher" once "knowledge" implicates them in the content. That is, once they have knowledge of the defamation, their own action of distribution becomes a "re-publication" subjecting them to liability as if they had been the original publisher.

Note that it is under this kind of analysis that the Zeran court refused to find a distinction between publisher and distributor for purposes of CDA §230:

> "Zeran simply attaches too much importance to the presence of the distinct notice element in distributor liability. The simple fact of notice surely cannot transform one from an original publisher to a distributor in the eyes of the law. *To the contrary, once a computer service provider receives notice of a potentially defamatory posting, it is thrust into the role of a traditional publisher*." Zeran at 332. [emphasis added]

While we agree with the court's analysis on this point, we disagree with application of this proposition to provide blanket immunity to ISPs under CDA §230. Cf. Ehrlich, supra footnote 59.

66 See Restatement (Torts) §577(2) "One who intentionally and unreasonably fails to remove defamatory matter that he knows to be exhibited on land or chattels in his possession or under his control is subject for its continued publication."

67 See Heller v. Bianco, 244 P.2d 757 (1952).

68 Note that the owner is under no duty to "police" or otherwise screen for such acts or to make inquiries. The duty arises solely on notice and the duty is to exercise reasonable care to abate. Restatement (Torts) §577(2) Comment on Subsection (2).

Copyright

Copyright law grants to the copyright holder certain exclusive rights. [FN 69] A person who violates any one of these rights is guilty of infringement. [FN 70] Although the Copyright Act "does not expressly render anyone liable for infringement committed by another," under certain circumstances, third parties are held liable for the infringing act of another under the doctrines of vicarious and contributory infringement. [FN 71]

To find secondary liability requires that there first be a primary infringement. [FN 72] In some cases of secondary liability, direct liability for infringement can also be found where the third part exercises one of the exclusive rights directly. A finding of direct infringement requires "some element of direct action or participation." [FN 73] This requirement can be seen as analogous to the "editorial participation" requirement for distinguishing between publisher and distributor liability in defamation. [FN 74]

So, in cases involving copyright and bulletin board service ("BBS") operators, courts have found liability in cases where the BBS encouraged members to upload files and used a screening procedure to determine what files could be uploaded [FN 75], and refused to find liability in a case where the BBS did not control or monitor the content. [FN 76]

---

69 Copyright Act, 17 U.S.C. §§101 et seq. (1998). Exclusive rights are set out in §106.

70 See 17 U.S.C. §501. "Copying" is a judicial shorthand for infringement. See Playboy v. Webbworld, 991 F. Supp. 543, 550-551 (N.D. Texas December 1997).

71 Sony v. Universal City Studios, 464 U.S. 417, 434-435 (1984). Cf. patent law, 35 U.S.C. 271(b) ("Whoever actively induces infringement of a patent shall be liable as an infringer.") and 35 U.S.C. 271(c) (defining liability for contributory patent infringement).

72 Sony, supra footnote 71, at 434. And, no affirmative defense of "fair use" under 17 U.S.C. §107. In general, the courts have held that there cannot be a finding of "secondary" liability where there is no primary infringement. Although beyond the scope of this paper, we question whether new communication technologies challenge this principle also.

Query for another forum: If a third party links to a "fair use" but charges for such access are they liable for infringement of the original copyright? For example, in the context of a critical review, a newspaper web site posts an excerpt from the reviewed work (arguably fair use). Another web site that charges for access to such works hyperlinks to the newspaper's posting. Does the hyperlink infringe the original copyright even though it "copies" a fair use? Under our analysis, the third party would be directly liable and the intervening fair use would not change the responsibility base for the ultimate harm. However, it is not immediately apparent how a court that required the showing of a primary infringement would analyze this situation.

73 Playboy v. Russ Hardenburgh, 982 F. Supp. 503, 512 (N.D. Ohio 1997).

74 See text accompanying footnotes 52 through 68 supra.

75 Playboy, supra footnote 73.

76 Religious Technology Center v. Netcom, 907 F. Supp. 1361, 1368-1370 (N.D. Ca. 1995). But cf. Playboy v. Frena, 839 F. Supp. 1552, 16555-1559 (M. D. Fl. 1993) (holding BBS operator liable for copyright infringement for failing to prevent users from uploading illegal copies of Playboy photographs, despite any evidence of prior knowledge), superceded by statute (Title II of the Digital Millennium Copyright Act "DMCA" of 1998, 17 U.S.C. §512), see ALS Scan v. RemarQ Communities, supra footnote 13, 239 F.3d 622 (holding that the DMCA codifies the Netcom principles).

The DMCA is discussed in Part IV, infra.

Vicarious Liability.

Vicarious liability arises under the common law doctrine of agency – *respondeat superior* – the responsibility of the superior for the acts of their subordinate. [FN 77] As discussed above in Part I above, under our constitutive analysis of responsibility, this equates to the "spatial extension of self". [FN 78]

The concept of vicarious liability in copyright cases is delineated in two lines of cases known as the "dance hall" cases (in which dance hall operators are held liable for infringement by bands performing copyrighted works in their establishments) [FN 79] and the "landlord" cases (in which no liability is imposed on landlords who merely lease space at fixed rates and who have no knowledge or control over the lessee's infringing activity). [FN 80]

Vicarious liability can be established where the third party has (i) the right and ability to control, and (ii) a direct financial interest in the use. [FN 81] Thus, vicarious liability has been found in cases of trade show organizers who exercised control over their exhibitors but not where the organizers did not. [FN 82]

In the context of online services, the question of control often turns on the same analysis discussed in the Cubby and Stratton Oakmont defamation cases above, that is, did the third party exhibit the requisite "control" by participating in the "editorial process". [FN 83].

The second requirement of vicarious liability – "a direct financial interest" – has been satisfied where the third party had a direct interest in the sale [FN 84] or the performance [FN 85]. Further, in Fonovisa v. Cherry Auctions [FN 86] the operator of a swap meet was found vicariously liable for vendor infringement although there was no direct link between the sale and the owner's profit.

---

77 See Restatement (Second) of Agency, §220 (1958).

And see Demetriades v. Kaufmann, 690 F. Supp. 289, 292 (S.D. N.Y. 1988):

> "it appears that two avenues of third party liability in copyright have grown up in the law – "vicarious liability" (grounded in the tort concept of *respondeat superior*) and "contributory infringement" (founded on the tort concept of enterprise liability)."

78 See text accompanying footnotes 28 through 31 supra.

79 See Dreamland Ballroom v. Shapiro, Bernstein, 36 F.2d 354 (7 Cir. 1929) (dance hall hired band to play music for paying customers) and Shapiro, Bernstein v. H.L. Green, 316 F. 2d 304, 307-308 (2d Cir. 1963) (citing relevant cases). See also, footnote 18 in Sony, supra footnote 69, at 437.

80 See Deutsch v. Arnold, 98 F2d 686 (2d Cir. 1938). And see Rebecca Morris, "Note: When is a CD Factory Not Like a Dance Hall?" 18 Cardozo Arts and Entertainment L. J. 257, 287-294 (2000). See also, footnote 18 in Sony, supra footnote 71, at 437.

81 Shapiro, Bernstein, supra footnote 79, 316 F.2d at 307.

82 Compare Polygram v. Nevada/TIG, 855 F. Supp. 1314 (D. Ma. 1994) (finding liability) with Artists Music v. Reed Publishing, 31 U.S.P.Q.2d 1623 (S.D.N.Y. 1994) (finding no liability).

83 See, for example, Netcom, supra footnote 76, at 1376 (requisite control is an issue of fact).

84 See Shapiro, Bernstein, supra footnote 79, 316 F.2d at 308-309 (storeowner received percentage of direct infringer's receipts).

85 See Dreamland Ballroom, supra footnote 79 (ballroom charged admission).

86 76 F.3d 259, 262-263 (9th Cir. 1996).

The standard set forth in Fonovisa is whether the presence of the infringing activity – either sales or performance of infringing material – on the third party's premises makes the business more attractive to customers and thus more lucrative to the third party. [FN 87]

The courts have applied the Fonovisa test in cases involving ISPs and web sites that charge users flat-rate pricing for access, distinguishing between the two types of 'service'. In Religious Technology Center v. Netcom, involving an ISP, the court found no credible evidence in the record that the infringing content posted increased the value of Netcom's service or attracted new customers nor that there was any measurable benefit from its policy of not policing content. [FN 88] The court held that there was no "direct financial interest". [FN 89]

However, in Playboy Enterprises v. Webbworld, the court found that a web site operator was closer to the infringement (although knowledge is not a requirement under vicarious liability) and the presence of infringing material increased the attractiveness of the site for new customers and thus the owner received a financial benefit despite a flat fee. [FN 90]

We do not believe that a categorical distinction between ISP and web site operator (nor a distinction between hosting and ownership) should necessarily be dispositive of the 'financial interest' test under Fonovisa. For example, a sophisticated application of that test in the case of ISPs might distinguish among different access providers by how the infringing activity drove demand for the underlying service itself.

So, for example, although financial interest was not at issue in RIAA v. Verizon [FN 91] it could be argued that Verizon and other DSL providers derive direct benefit from the demand for broadband stimulated by illegal file trading, while cable operators supplying cable modem service do not. [FN 92] Further, in this particular case, Verizon also derives market benefit by resisting copyright enforcement. [FN 93]

---

87 Ibid. at 263.

88 Netcom, supra footnote 76, at 1377.

89 Ibid.

90 Playboy Enterprises v. Webbworld, 968 F. Supp. 1171, 1175-1177 (N.D. Texas 1997). Compare Marobie-FL v. NAFED, 45 U.S.P.Q.2d 1236 (N.D. Ill. 1997) holding that a hosting service was not liable for web content where the hosting fee was fixed and did not vary based on traffic to the infringing material.

91 RIAA v. Verizon, D.C.D.C. 02-MS-0323-JDB, decided January 21, 2003.

92 Compare Verizon's position as a supplier of DSL service providing dedicated bandwidth with that of cable modem service operators providing shared bandwidth service. Peer-to-peer networks ("file sharing" or "pirate" applications depending on which side you are on) use significant bandwidth. For suppliers of dedicated bandwidth, i.e. the phone companies providing DSL Internet service, high bandwidth applications create additional demand for service, that is, more DSL lines. For suppliers of shared bandwidth, i.e. the cable operators ("MSOs") providing cable modem Internet service, peer-to-peer bandwidth demands degrade service for other users sharing the same bandwidth.

Naturally then cable operators are clamping down on peer-to-peer network usage but DSL suppliers are not. Hence, Verizon's position in RIAA v. Verizon can be seen as protecting its business model, and, in our view, would justify a finding of "direct financial interest" under Fonovisa. Cf. Netcom, supra footnote 76 at 1377, where the court found the record lacking in evidence of financial effect.

With respect to peer-to-peer networks and cable modem Internet service providers, see "Studios Waging Web War," at http://www.eonline.com/News/Items/0,1,10309,00.html and "Fowl Snip," Village Voice, August 12, 2002 at http://www.villagevoice.com/issues/0233/koerner.php (both about Time Warner Online restricting bandwidth for peer-to-peer service) and see "Peer-to-Peer Gets

Contributory Liability

The doctrine of contributory liability is rooted in the tort theory of enterprise liability, which we would describe as implicating the 'social self'. [FN 94] Contributory liability is imposed on "activities that make such [infringement] possible." [FN 95] In Gershwin v. Columbia Artists, the Second Circuit set out the standard for contributory liability:

> "One who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another may be held liable as a 'contributory' infringer." [FN 96]

The key elements for contributory infringement are knowledge and material contribution. [FN 97]

Under Fonovisa, supplying the "site and facilities" for direct infringement is "materially contributing" to the infringing conduct of another. [FN 98] And, under Netcom, "failure to cancel [a user's] infringing message and thereby stop the infringing copy from being distributed worldwide constitute substantial participation." [FN 99] However, Sony v. Universal Studios, rejected the proposition that "merely provid[ing] the means to accomplish an infringing activity" was sufficient without constructive knowledge of the infringing activity. [FN 100]

The additional requirement for contributory infringement is knowledge – the secondary infringer must "know or have reason to know" of direct infringement. [FN 101] In Napster, the court

---

Pummeled," in "Looks Like a Tough Year Ahead for Cable IP," in Cable Datacom News, January 2003, available at http://www.cabledatacomnews.com/jan03/jan03-2.html (generalizing the peer-to-peer problem for MSOs).

93 Comments made by John Thorne, SVP and Deputy General Counsel, Verizon, January 2003, Columbia Law School (claiming that Verizon was getting "good press" and attracting new customers for "protecting user privacy" against the RIAA). Cf. Netcom, supra footnote 76 at 1377, where the court found no evidence of a measurable benefit to Netcom from its policy of not policing the content on its systems.

94 See Demetriades v. Kaufmann, 690 F. Supp. 289, 292 (S.D. N.Y. 1988) :

> "it appears that two avenues of third party liability in copyright have grown up in the law – "vicarious liability" (grounded in the tort concept of *respondeat superior*) and "contributory infringement" (founded on the tort concept of enterprise liability)"

And, see text accompanying footnotes 38 through 41 supra, discussing constitutive responsibility and the extension of 'self' along the social dimension.

95 Sony, supra footnote 71, at 442.

96 Gershwin Publishing v. Columbia Artists Management, 443 F.2d 1159, 1162 (2d Cir. (1971).

97 See A&M Records v. Napster, 239 F.3d 1004, 1020-1022 (9th Cir. 2001).

98 See Napster, supra footnote 97, at 1022. See also Netcom, supra footnote 74, at 1374 (incorrectly cited in Napster as "1372").

99 Netcom, supra footnote 76, at 1374 (incorrectly cited in Napster, supra footnote 92, at 1022 as "Netcom … at 1372").

100 Sony, supra footnote 71, at 436, 439.

101 Napster, supra footnote 97, at 1020. And, see footnote 76 supra, and discussion in Part IV infra, regarding the codification in DMCA §512 of a 'knowledge' requirement.

refused to "impute the requisite level of knowledge to Napster merely because … [the] technology may be used to infringe … copyrights." [FN 102] Nevertheless, the court in Napster concluded that sufficient actual knowledge existed to impose contributory liability. [FN 103]

Employer Liability under the Doctrine of *Respondeat Superior*.

Traditionally, in order to find employer liability under the doctrine of *respondeat superior*, it was required to show that the conduct in question was "within the scope of employment." [FN 104] This requirement that conduct be "within the scope" of employment, puts employer liability squarely within the extension of the 'spatial self' as discussed above. [FN 105]

However, courts have significantly expanded employer liability beyond this traditional formulation:

> One rationalization for this [expanded view] is that since the employee's job created the opportunity for the employee to commit the wrongful or illegal act, and gave the employee apparent authority, the employer therefore possessed the requisite element of control. In other words, the employer has more or less fictitious control over the employee, and therefore, [liability]" [internal quotations and citations omitted] [FN 106]

Although couched in terms of "control" in the above-quoted material, for our purposes, we suggest that this broader formulation extends liability from the narrower 'spatial extension' (direct control) to the 'social extension' of constitutive responsibility. That is, the employee comes within the expanded social self or corporate identity of the employer because it is that status that creates the opportunity for the wrongful conduct to have effect. The responsibility base is the joint participation – the social construction – entered into between the employer and the employee that gives the conduct effect, rather than a stretched notion of "fictitious control".

Part II Summary

We summarize here some observations of common elements underlying these doctrinal approaches to third party liability:

As a general matter, third party liability arises where there is some nexus to the primary conduct and either:

(i) material participation in or control over the initiation of the conduct,
(ii) knowledge of the conduct and control over the cessation of the conduct, or

---

102 Ibid. at 1020-1021. (stating "We are bound to follow Sony, and will not impute …")

103 Ibid. at 1021-1022. ("The record supports the district court's finding that Napster has actual knowledge that specific infringing material is available … ").

Note that the court in Napster also "declines to apply the staple of commerce doctrine [from Sony, supra note 71, at 490-491] because … Napster exercises ongoing control over its service." The staple article of commerce doctrine (under which there is no liability for introducing a staple article into the stream of commerce) is only applicable where there is no ongoing relationship between the provider of the article and the staple or the user. Thus, such doctrine is not applicable to ISP liability and we do not discuss it further here.

104 See Restatement (Second) of Agency § 228 (1958). See also the discussion of the "spatial extension of self," supra text accompanying footnotes 29 through 31.

105 See text accompanying footnotes 28 through 31, supra.

106 Mark Ishman, "Computer Crimes and the Respondeat Superior Doctrine: Employers Beware," 6 Boston Univ. J. Science and Technology Law 6 (2000) at II (B) (15).

(iii) a financial or social interest or benefit from association with the conduct.

Although there is fluidity among categories in any conceptual taxonomy, for analytic purposes here, we can ascribe liability to a third party by extending the boundaries of the third party 'self' or identity along the 'spatial' dimension under (i) above, along the temporal dimension under (ii), and along the social dimension under (iii). [FN 107]

Another way to classify third party liability might be to consider 'vicarious' responsibility as primary liability (where the act of another is attributed to the third party as if the conduct were the act of the third party) by virtue of the relationship with the actor [FN 108] and 'contributory' responsibility as 'secondary' liability (for the primary act) by virtue of the third party's relationship with the actual harm (either by enabling it or benefiting from it). [FN 109]

Under a paradigm of constitutive responsibility, vicarious liability derives from object-responsibility, and contributory liability derives from subject-responsibility. [FN 110]

PART III. Performative Effect, Illocutionary Force, and Constitutive Responsibility.

From the previous section, the obvious is confirmed – that is, the circumstances under which one party is held legally accountable for the conduct of another is dependent on the relationship of the third party to the actor or the conduct. In this section we explore an analytic framework for assessing that relationship based on its *performative* characteristics.

Technological systems, together with the rules and conventions that govern human interaction with them, can be viewed as acts of social construction. [FN 111] As a technological system for "worldwide human communication" [FN 112], cyberspace can be viewed as a large semiotic act [FN 113] – that is, as an ongoing conversation or social symbolic act. [FN 114].

---

107 See text accompanying footnotes 28 through 41, supra.

108 The actor's self is subsumed in the third parties identity, for example, under the doctrine of *respondeat superior*.

109 The actual harm itself comes within the boundaries of the third party's identity.

110 But cf. Sony, supra footnote 71, at 435, where the court uses the term 'vicarious liability' broadly to included contributory liability:

> "[V]icarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances under which it is just too hold one individual accountable for the actions of another."

111 On the general topic of social construction and technological innovation, see Wiebe E. Bijker, Thomas P. Hughes, and Trevor Pinch, eds. "The Social Construction of Technological Systems," Cambridge: MIT Press (1994, 1987) and Wiebe E. Bijker and John Law, eds. "Shaping Technology/Building Society," Cambridge: MIT Press (1992).

112 Reno, supra footnote 2, at 850.

113 Semiotics concerns itself with the construction of meaning from signs and systems. See generally, Umberto Eco, Semiotics and the Philosophy of Language," Bloomington: Indiana University Press (1984), Roland Barthes, "Elements of Semiology," Noonday Press (reissue 1977), de Saussure, infra footnote 36, and Blonsky, infra footnote 31. Although derived from linguistics, semiotics can be understood as the study of all meaning derived from any system. See, generally, Floyd Merrell, "Semiosis in the Postmodern Age," West Lafayette: Purdue University Press (1995).

A useful analytic tool for determining responsibility for semiotic acts can be found in John L. Austin's exposition of "speech-act" theory. [FN 115]

Speech act theory is the analysis of language by what it does through social process rather than what it represents through formal structure. [FN 116] Speech-act theory examines the power of language in community, that is, as it is used to do things, not just to say things.

Austin distinguishes language with the primary function of doing something – "performative" speech acts – and language used primarily for saying something – "constative" speech acts. [FN 117]

For example, in the context of cyberspace, "the information is available on my web site" is constative but the statement "<A HREF="http://www.taipale.com/info_here/">Click Here for Information</A>" is performative. Much of legal language is performative, for example, "you are negligent" assigns responsibility and has social consequence.

However, the ability of performative speech to do something is contextual. Thus, the statement that "you are negligent" has significant different effect if uttered by a person on the street or by a judge in a courtroom. [FN 118] So too, the hyperlink described in the previous paragraph is performative only in context, that is, when embedded in an HTML document.

Importantly, performative communication cannot be judged as true or false but only as effective or not. [FN 119] The concept of a communication's effectiveness is related to what Austin calls its illocutionary force. Again as example, the words "the constitution is suspended" appearing in a governmental decree or in a newspaper editorial are examples of a single *locution* with very different *illocutionary* force. "The same words with the same meaning – the same locutions – have different conventional powers, and one of the most important principles of speech-act theory

---

114 See K. A. Taipale, "Free Speech, Semiosis, and Cyberspace: The Hyperlink as Nexus to Felicity," available at http://www.taipale.com/papers/CyberSemiosis.pdf. And, see generally Roman Jakobson, "Main Trends in the Science of Language," New York: Harper (1970) and Roland Barthes, Jacques Derrida, Umberto Eco, Michel Foucault, Milton Glaser, Frederic Jameson, Thomas Sebeok, and others, in Marshall Blonsky, ed., "On Signs," Baltimore: Johns Hopkins University Press (1991, 1985).

Compare this social semiotic view of cyberspace with a more simplistic view of online communication as the act of acquiring information. See generally Claude E. Shannon and Warren Weaver, "The Mathematical Theory of Communication," Urbana: University of Illinois Press (1949). Shannon developed the mathematical theory of signal transmission while a researcher at Bell Labs and professor at MIT. Digital communication technology – that is, cyberspace itself – is a direct result of Shannon's work in information theory.

115 See John L. Austin, "How to Do Things with Words," Cambridge: Harvard University Press (1962) and John R. Searle, "Speech Acts: An Essay in the Philosophy of Language," New York: Cambridge University Press (Reprint edition 1999, 1969).

116 See Sandy Petrey, "Speech Acts and Literary Theory," New York: Routledge (1990), pp. 3-21. Compare this with traditional linguistic research that focuses on abstract structural features of language independent of where and when it is used. See, for example, Ferdinand de Saussure, "Course in General Linguistics," New York: McGraw Hill (1965, 1916)

117 Austin, supra footnote 115, at 6.

118 The converse obviously also holds, that is, the same context but different language can have significant difference in effect. For example, the significant social difference between the judicial performative "case dismissed" and "twenty years". Petrey, supra footnote 116, at 8.

119 Ibid. at 12.

is that such difference of power is at least as important in analyzing language as lexical and semantic differences". [FN 120]

Thus, in the context of secondary liability, third party liability can be analyzed by examining the illocutionary force of the primary act that is attributable to the relationship of the third party to the primary actor or conduct. The third party incurs responsibility for its own act of providing contextual effectiveness to the primary conduct.

So, for example, the court in Napster finds "the global scale of Napster usage … militates against a determination that … [use] constitutes personal or home use in the traditional sense." [FN 121] Conduct that might have been permissible at home gains illocutionary force by virtue of the Napster service. Napster is held liable for contextualizing the individual user behavior in a way that creates or gives effect to the social harm.

Generalizing the same analysis, ISPs can be judged by the relationship of the service provided to the actual harm resulting from the conduct of their users. Such constitutive responsibility can be related directly to the illocutionary effect that their own conduct gives to the primary act of misconduct – the ISP is subject-responsible for providing the enabling context.

Importantly, however, like performative speech generally, the performative effect of the ISP service is not judged right or wrong (i.e., true or false) but only by its effectiveness in allowing the primary conduct to have harmful effect. Thus, there should be no attempt to ascribe culpability for the service itself, only for the effect of such service in context of the actual harm.

Therefore, because such a responsibility base is related to particular effect (and not intent or other "bad motive" in providing service) legal liability should only accrue for mitigating ongoing harm – not for the primary act alone unless there is an independent responsibility base for primary liability – either actual control or perhaps reckless disregard. [FN 122]

---

120 Petrey, supra footnote 116, at 12, and see "The Structure of Illocutionary Acts," in Searle, supra footnote 115, at 54-71.

121 Napster, 114 F. Supp. At 914.

122 Such a standard would be akin to that applied in defamation cases where the third party has control of the instrumentality (see footnotes 66-68 supra and accompanying text) but their duty to "police" is circumscribed, or that applied under contributory infringement of copyright for finding material contribution (see text accompanying footnote 99, supra, quoting Netcom) once knowledge has been established.

PART IV. Applying a Constitutive Standard for Third Party Liability

Deterrence theory seeks to impose the social cost of misconduct on the responsible party. [FN 123] The standard economic theory of deterrence would ascribe the full social cost of harms on primary wrongdoers in order to force internalization of the costs of their conduct. [FN 124] Strict liability is generally preferred because "it not only provides defendants with optimal incentives to prevent misconduct, but also ensures that defendants will adopt an optimal level of activity." [FN 125]

In reaching for third party liability for ISPs, most commentators argue that the structure of the Internet makes imposing responsibility directly on users difficult or costly and, therefore, third party liability should be extended to those parties in a position to prevent the social harm at a reasonably low cost. [FN 126] However, in the case of third party liability, imposition of the full social cost through a regime of strict liability results in deadweight losses or overdeterrence because the third party bears the full cost of the social harm but is unlikely to capture the full value of the conduct, thus, they are likely to adopt excessively restrictive policies. [FN 127]

For example, holding an ISP strictly liable for the full cost of the harm of copyright infringement by users participating in peer-to-peer file sharing networks is likely to create an incentive for overdeterrence. The ISP does not capture the value of the use of the peer-to-peer network – neither the benefit of the illegal use nor the benefit for alternative legal uses – the user does. [FN 128] In addition, the ISP would incur high monitoring costs to discriminate between illegal and legal uses. [FN 129] Thus, strict liability would impose an incentive to terminate service regardless of the loss of value to the users (or society). [FN 130]

---

123 Hamdani, supra footnote 14, at 910.

124 Ibid., at 913 and footnote 43 therein.

125 Hamdani, supra footnote 14, at 904, and footnote 11 therein citing Steven Shavell, "Strict Liability Versus Negligence," 9 J. Legal Studies 1, 2-3 (1980) and Hamdani at 913-914 and footnote 43 therein.

But, cf. Nicholas Mercuro and Steven G. Medema, "Economics and the Law: From Posner to Postmodernism," Princeton: Princeton University Press (1997), pp. 71-74, contrasting the "Chicago school" perspective (negligence is preferred standard as it minimizes overall social cost associated with risk) with the justice/fairness approach (strict liability lowers the cost to the victim by shifting more to the injurer).

126 Hamdani , supra footnote 14, at 911. And, see Reinier H. Kraakman, "Corporate Liability Strategies and the Costs of Legal Control," 93 Yale L. J. 857, 888-896 (1984) third party liability required to avoid underdeterrence through enforcement failures), also cited in Hamdani at footnote 31 and 33 therein.

127 Hamdani, supra footnote 14, at 905, 916-918. Hamdani develops an "incentive-divergence" thesis to explain why strict liability should not be applied to ISPs because to do so "would induce them to adopt excessive levels of monitoring and employ overly zealous censorship policies." Cf., however, Ronald H. Brown and Bruce Lehman, Information Infrastructure Task Force, "Intellectual Property and the National Information Infrastructure," (1995) at pp. 114-1124, describing the need for strict ISP liability for user copyright infringement.

128 But see footnote 92 supra (discussing how DSL service providers benefit from illegal file sharing applications on their network).

129 See Niva Elkin-Koren, "Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators," 13 Cardozo Arts & Ent. L. J. 345, 406

Strategies of Third Party Liability

ISPs have exclusive technical control over user conduct and absolute technical control to prevent user misconduct by denying or blocking access to network services. Such third party 'gatekeeper' control can implicate three enforcement strategies – monitoring for prevention of misconduct, blocking or removing to prevent ongoing misconduct, and whistleblowing. [FN 131]

Monitoring

Commentators have generally discarded strict liability for ISPs because of the prohibitive cost of monitoring user activity. [FN 132] However, conventional economic theory would hold that high monitoring costs should not, in themselves, preclude adoption of strict liability because internalizing such costs and weighing them against the potential benefits and liabilities from a particular risk would lead to an optimal (economic) level of activity. [FN 133]

But, this outcome only prevails within the paradigm of primary liability. In cases of secondary liability, because of the "incentive-divergence" between the potential liability of the ISP and the capture of benefits by the user, high monitoring costs coupled with strict liability are likely to result in significant overdeterrence. [FN 134] The optimal strategy for an ISP will be to eliminate significant amounts of legal conduct or service from its network in order to avoid incurring monitoring costs that would be required to distinguish between illegal and legal conduct and to avoid liability costs that would result from any misconduct that was not prevented.

Imposition of knowledge-contingent standards avoids overdeterrence, however, such standards tend to encourage ISPs to ignore user misconduct. [FN 135] Thus, some commentators have argued that knowledge-contingent standards should only be introduced in conjunction with monitoring regulations. [FN 136] Under monitoring regulations, lawmakers set the optimal level of monitoring and ISPs that satisfy such standards will not be held liable. [FN 137]

(1993) (incorrectly cited in Hamdani, footnote 49 therein, as "1995") ("the cost of monitoring and the risk of liability may also reduce the incentives of BBS operators to provide on-line services").

130 See Hamdani, supra footnote 14, at 905-906. See also footnote 127 supra.

131 Reinier H. Kraakman, "Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy," 2 J. L. Econ. & Org. 53 (1986). And see Katyal, supra footnote 12, at 1094-1100.

132 Hamdani, supra footnote 14, at 914:

> "Invoking the prohibitive cost of monitoring user conduct over the Internet, commentators have commonly discarded strict liability as unsuitable for the ISP industry. The argument against strict liability is basically the following: While some users indeed abuse their Internet access for committing misconduct, the majority of users rely on their Internet access to engage in legitimate activities. ISPs are unable to distinguish between legitimate and illegitimate user conduct without monitoring information disseminated through their networks. The voluminous amount of data transmitted through the Internet makes such monitoring very costly. Strict liability, therefore, is undesirable because it fails to take into account the high cost of monitoring." [citations omitted]

133 Ibid., at 915.

134 Ibid., see generally Part I (C) and Part II. And, see footnote 15 supra.

135 So-called "willful blindness".

136 Hamdani, supra footnote 14, at 936.

137 Ibid., at 933-934. Compare the procedural standards in the DMCA discussed infra.

However, any such monitoring-regulation regime is likely to suffer from (i) inflexibility in that such a regime imposes a uniform standard on performance regardless of particular conditions, costs or relative benefits in a particular situation (or for a specific service), (ii) a tendency to establish a floor (or ceiling) for performance and "lock in" a set level of performance, and (iii) discouragement of technical innovation (no incentive to innovate beyond existing standards). [FN 138]

For these reasons, legislative standard setting for monitoring online conduct is particularly inappropriate in areas of rapid technical innovation. Any standard for compliance is likely to be obsolete when enacted since it will not take into account innovations in services, monitoring technologies, or user behaviors. [FN 139]

In order to avoid overdeterrence and prevent willful blindness, we propose that the guiding principle for third party ISP liability be negligence [FN 140] based on the constitutive responsibility base of the ISP for the particular conduct at issue. [FN 141] We would encourage Congress to develop statutory procedural guidelines, somewhat like those in the DMCA discussed below, in particular doctrinal areas of concern but not set explicit monitoring or technical requirements.

In the absence of legislative action in any particular area we would propose that the courts apply a reckless or willful standard for monitoring or discovering misconduct, that is, an ISP would only be liable for conduct of which they were unaware where it was found reckless or willful to provide such service or allow such conduct without effective monitoring or other preventative measures that were particular to the service and the technology being offered. For example, liability might be imposed even without specific knowledge in situations where the technical means for monitoring were available and cheap, the conduct easy to detect, and the harm great.

In line with the analysis developed elsewhere herein, the court would look to such factors as the ease and cost at which behavior could be monitored or discovered, the relative harms of the particular conduct, the relative benefit of the service provided, and the reasonableness of technological choices made by the ISP in providing services. In all cases, these factors would be weighed against the performative effect of the third party's constitutive responsibility base. In

---

138 Any system of legislated technical standards is subject to the same criticisms that are leveled at the current "command-and-control" standard setting regime employed in environmental regulation. See generally the text accompanying footnotes 45-54 in K. A. Taipale, "Information Technology as Agent of Change in Environmental Policy," available at http://www.taipale.com/papers/AgentofChange.pdf .

139 Not only will new innovation outpace legislative standard setting, but technological innovation will be directed specifically at circumventing such standards much like the development of second generation peer-to-peer networks such as Morpheus and Kazaa were developed to circumvent the "standards" for liability set forth in Napster.

140 Note that the "Chicago school" approach to law and economics favors rules that lower overall social costs. Compare the more traditional justice/fairness approach that is concerned with the distribution of costs between compensated risk and background (or assumed) risk (that is, between injurer and victim). In the case of ISPs, one could argue that a negligence rule would result in lower overall social costs of enforcement because it would eliminate the high cost of monitoring that would be required under a strict liability standard. See generally, Mercuro, supra footnote 125, at 72-73.

141 Some commentators have argued that in an area of rapid technological change, regulation may be better than negligence as an enforcement strategy because in applying a negligence standard to newly emerging technologies and services, courts are likely to reach contradictory results thus decreasing certainty for potentially responsible parties and increasing the possibility for over deterrence as ISPs reduce their potential exposure by engaging in excessive monitoring or denial of service. See Hamdani, supra footnote 14, at 935. But see 936 , "On the other hand, the rapid pace of technological change might make negligence superior to regulation." (Citing possible obsolescence of regulation and greater flexibility of negligence.)

order to avoid overdeterrence we would propose a presumption of immunity without a showing of reckless disregard (or "willful blindness") (absent actual or constructive knowledge).

Blocking or Removing

Under conditions of "willful blindness" or where there is actual or constructive knowledge of the illegal conduct, ISPs should be held to a duty to exercise reasonable care to abate the illegal conduct. [FN 142] Again, the inquiry would be specific to the circumstances, including the nature and technical characteristics of the service provided and its performative effects, as well as the particular type and severity of the harm. So, as discussed above [FN 143], access service providers might be held to a different standard depending on whether they were offering DSL or cable modem internet access, or where the illegality was easily assessed (for example, copyright) or more difficult (for example defamation). [FN 144]

Whistleblowing

Whistleblowing, that is, the reporting of illegal conduct, should be required under the same conditions as blocking access or removing material, that is, where the ISP has actual or imputed knowledge of the illegality they should be under a duty to report such conduct to the appropriate authorities. [FN 145]

Digital Millennium Copyright Act of 1998

Congress enacted §512 of the DMCA [FN 146] to limit ISP liability for copyright infringement by their users by creating a series of "safe harbors" for ISPs that might have been held liable for copyright infringement under traditional doctrines. [FN 147] These safe harbors depend on the type of service offered – transitory network communications, system caching, storage of information at the direction of the users, and information locating tools – and set different requirements for each type.

We do not intend here to review all of the provisions of the DMCA. In general, the DMCA follows certain of the suggestions set forth above and attempts to avoid overdeterrence while providing effective enforcement by directly regulating the relationship among the ISP, the user and the copyright holder. The DMCA provides procedures that shift the cost burden of detecting copyright infringement to the copyright holder, provide specific procedures for notifying the ISP of infringing activity [FN 148], procedures for the ISP to follow upon notice (removal and notice to the affected user) [FN 149] and immunity for actions taken in conformity with these procedures. [FN 150]

---

142 See generally footnotes 66-68 and the accompanying text.

143 See footnote 92 supra.

144 See also footnote 27 supra.

145 Note that under 42 U.S.C. §13032 (Lexis 2003) ISPs currently have a duty to report incidents of child pornography that they become aware of. §130329(c) provides civil immunity to ISPs for good faith reporting under this section, and §13032(e) provides that "monitoring is not required".

146 17 U.S.C. §512 (Lexis 2003).

147 See text accompanying footnotes 69-108 supra.

148 17 U.S.C. §512(c)(3).

149 17 U.S.C. §512(c)(1)(C).

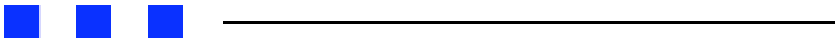
150 17 U.S.C. §512(g).

Part IV Summary

ISPs should be held liable for the misconduct of their users under a paradigm of constitutive responsibility measured in terms of the performative effect (illocutionary force) that their provision of service gives the misconduct.

In order to prevent overdeterrence, however, liability should generally only be imposed under knowledge-contingent circumstances. But, in order to avoid encouraging "willful blindness" on the part of ISPs to illegal activity by their users, there should be liability where failure to monitor or prevent the primary act constitutes reckless or willful conduct in the particular circumstances. In considering the circumstances, the court should evaluate the particular service offered, the characteristics of the illegal behavior and the state of the available technological art in monitoring or controlling such behavior.

ISPs with actual or imputed knowledge should be required to exercise reasonable care to abate the conduct by removing material or blocking access.



PART V. Conclusion: A Research Agenda

This paper has explored third party liability under various theoretical constructs, including a constitutive paradigm for responsibility, existing legal doctrines of secondary liability, and a performative evaluation of effect. In Part IV we put forward a tentative framework for applying a performative standard for constitutive responsibility on ISPs for user misconduct based on negligence. However, this paper is not intended to be a definitive statement of these issues, but rather a preliminary research agenda delineating certain areas for further exploration.

Cyberspace has the potential to be a great liberating forum for human expression or an abyss of human avarice filled with pornography, defamatory statements, stolen intellectual property, hate speech and other harmful things. In reality, it will probably be both.

Unlike realspace, however, cyberspace presents third party gatekeepers that have the technical ability to control user conduct and access to the network. Finding or developing legal theories under which to impose responsibility on such third parties without creating unwanted incentives for overdeterrence of desirable conduct is a difficult task.

It is our position articulated here that constitutive liability for such third parties can be imposed directly based on an understanding of the performative affect of providing services that enable user misconduct to result in social harm.