2005

The Failure of the Rule of Law in Cyberspace? Reorienting the Normative Debate on Borders and Territorial Sovereignty

H. Brian Holland

24 J. Comp. & Info. L. 1 (2005)
DRAFT

The Failure of the Rule of Law in Cyberspace? Reorienting the Normative Debate on Borders and Territorial Sovereignty

H. BrianHolland[1]

"[O]bservance of the rule of law is necessary if the law is to respect human dignity."

Joseph Raz [2]

Between 1996 and 2002, over the course of several law review articles, professors David R. Johnson, David Post, and Jack L. Goldsmith engaged in a highly influential debate addressing the significance and legitimacy of physical, geographically-defined borders and territorial sovereignty in the regulation of cyberspace.[3] At bottom, it was a contest between internal or "indigenous" regulation and the imposition of existing external regimes.[4] At its heart lay two overarching areas of disagreement: First,

---

[1] Assistant Professor of Law, Barry University School of Law; LL.M., Columbia University School of Law, with honors; J.D., American University's Washington College of Law, summa cum laude. Many thanks to Dean J. Richard Hurt, who provided me with the opportunity to present an early draft of this article at the Young Scholars Workshop of the Southeastern Association of Law Schools. Thanks also to my colleagues at Barry University School of Law, particularly professors Barry Dubner, Mark Summers and Stephen Tropp, for their insightful comments. Finally, thanks to Sarah, Will and Ella for the most important things.

[2] Joseph Raz, The Rule of Law and Its Virtue, in The Authority of Law: Essays on Law and Morality 221 (Oxford University Press 1979, 2002).

[3] See David. R. Johnson & David Post, Law and Borders - The Rise of Law in Cyberspace, 48 Stan. L. Rev. 1367 (1996); David Post, Against "Against Cyberanarchy", 17 Berkeley Tech. L.J. 1365 (2002); Jack L. Goldsmith, Against Cyberanarchy, 65 U. Chi. L. Rev. 1199 (1998) [hereinafter Goldsmith I]; Jack L. Goldsmith, The Internet and the Abiding Significance of Territorial Sovereignty, 5 Ind. J. Global Leg. Stud. 475 (1998) [hereinafter Goldsmith II]. This is, of course, not to ignore the valuable contributions of other academics to these issues, which are far too numerable to recite here. I have simply chosen to focus on the Johnson-Post-Goldsmith debates both because of their notoriety and as a useful vehicle for reaching my primary points regarding the rule of law.

[4] See Goldsmith I, supra n. 3, at 1201 (although Professor Goldsmith protested that his sole purpose was to defend the feasibility and legitimacy of the regulation of cyberspace, and not to "take a position on the merits of particular regulations beyond their jurisdictional legitimacy," the debate into which he cast his hand was not nearly so narrow). See also Johnson & Post, supra n. 3, at 1367 (the very premise of Johnson and Post's article was that cyberspace "requires a system of rules quite distinct from the laws that regulate physical, geographically-defined territories," and that cyberspace should be allowed to "develop its own effective legal institutions.").

descriptively, whether and to what extent the architecture of the Internet is borderless or boundary-destroying, so as to be resistant to regulatory regimes grounded in territorial authority;[5] and second, normatively, whether and to what extent a nation may legitimately exercise its regulatory power extraterritorially, particularly in the context of online activity.[6]

Initially, this seemed a robust debate. Over time, however, that debate narrowed predictably. The descriptive issue moved from platitudes of the Internet's inherent nature to a contest of choices and predicted technological advancement. The normative question became fundamentally a disagreement about the origins and limits of sovereign power, particularly as related to the regulation of extraterritorial activities having local effects, as well as the spillover effects of such regulation. Related to this fundamental question, and particularly relevant here, the participants ultimately disagreed as to the legitimizing effect of jurisdictional and choice-of-law principles; i.e., whether these jurisprudential mechanisms for resolving regulatory overlap disputes adequately limit and resolve multiple, simultaneous, and competing claims of unilateral, extraterritorial regulatory power. This pushed the discussion back to the descriptive; to questions of functional identity, scale, effects, and (somewhat tangentially) consent. And here, it seemed to wither.

This article acknowledges these debates and their importance, but suggests that by framing the argument as they did, their authors - particularly Johnson and Post - were pressed to untenable assertions that fatally undermined their position. Seeking to avoid a similar fate, here the underlying issues are approached from a slightly different perspective. Jurisdictional and choice-of-law principles are recognized, fundamentally, as expressions of the rule of law; devices by which conformity to the rule of law is to be actualized. But the term "the rule of law" has recently become so commonplace and pedestrian that its precise connection to these principles may be lost.[7] Indeed, at times in their debate, professors Johnson, Post, and Goldsmith seem to talk around the rule-of-law concept,[8] failing to step back to adequately examine the purposes, values, and virtues of law from which their arguments might ultimately flow. My intent is to reestablish this link through consideration of the more fundamental question; whether the governance of cyberspace by traditional laws, imposed by territorially-based sovereigns, conforms to the rule of law. I conclude that the imposition of territorially-based regulatory regimes in the

---

5 Goldsmith I, supra n. 3, at 1203-04 (setting out the nature of the "skeptics" claims as a foundation for rebuttal).

6 Id. at 1204.

7 See e.g., David Kairys, Searching for the Rule of Law, 36 Suffolk U. L. Rev. 307 (2003) (providing a fascinating discussion of the use of the term "rule of law" in both legal and popular culture); See also Raz, supra n. 2, at 211 (arguing that many legal theorists, politicians, social commentators, and the like have made "promiscuous use" of the term "the rule of law.").

8 See e.g., Goldsmith I, supra n. 3, at 1203 (noting that "choice-of-law rules are thought to promote rule-of-law values like uniformity... predictability, and certainty," but failing to explore the import of the connection between these concepts).

governance of cyberspace fails to conform to the rule of law. But this is not the end of the inquiry. For if the rule of law fails in cyberspace, what then? Must we reform or recreate our regulatory system, or is conformity with the rule of law a less important virtue of legal systems than popular rhetoric might suggest?

It is important to acknowledge up front the obscurity of this task. Legal philosophy does not attempt to discern the law of a particular jurisdiction, but instead considers the law in general, seeking to isolate those attributes that are common to all legal systems. In seeking to elucidate and answer these questions, legal philosophers are inclined to avoid analysis of a specific legal system, allowing only an occasional reference for the sake of definitional clarity. Here, such avoidance is impossible, for the purpose of this article is to both describe a particular theory of normative jurisprudence - Joseph Raz's conception of the rule of law and its virtue - and to test various aspects of cyberspace governance, as it actually exists, for conformity to that normative ideal; i.e., what law ought to be.[9] Unifying abstract analytical questions about the nature of law and legal systems, their existence, content and validity, and normative questions about legitimacy, obligation, and justification, within the particularities of a specific legal construct, is itself a precarious undertaking. It is all the more problematic in this case, because conformity with the rule of law as an ideal would seem to presuppose the existence of laws as part of an identifiable legal system. Proving this presupposition and defining its margins is a potentially consuming enterprise that threatens to derail the central question. As such, I have set some initial parameters.

It is equally important to concede that this is not intended as a traditional work of legal philosophy, in the rather weighty sense of those words, but of the relationship between law and cyberspace. By necessity, issues, conceptions, and central arguments that have filled volumes are briefly summarized and often posited as settled questions, although nothing could be further from the truth. All this is to say that, in an attempt to reach a particular starting point for my discussion, I have paved over potholes and ignored forks in the road that others would find necessary to travel. I have done so, however, with the best intentions, taking pains to acknowledge points of greatest dispute where they occur.

The ultimate goal of this article is to suggest a different perspective on the issue of extraterritorial regulation in cyberspace. It is in no sense intended to exhaust the issue, even as to the impact of the rule of law on that analysis. I begin in Section I by outlining the normative debate on the governance of cyberspace, borders and territorial sovereignty, focusing on the Johnson-Post-Goldsmith debate. I then seek to identify

---

[9] Id. I can, no doubt, be roundly criticized for choosing to focus on a positivist conception of law, legal systems, and the rule of law, and for strictly limiting my frame of reference in evaluating conformity to the rule of law in cyberspace. And there is no question that these criticisms are in some sense well founded. Nevertheless, it bears repeating that the purpose of this rather short work is simply to introduce a new perspective on the extraterritorial regulation of cyberspace, and not to exhaust the field in attempting to defend what is a nascent thought.

weaknesses in this approach. This provides a foundation upon which to reframe the debate in Section II, moving from a focus on the validity of sovereign power and its limits, to the relationship between individual autonomy and the purposes, values and virtues of law. Here, the central question is whether the governance of cyberspace by traditional sovereign legal systems conforms to the rule of law. Answering this question in the negative, Section III asks simply, what then? Is conformity to the rule of law a prerequisite of authority or simply one value among many, to be weighed against other values served by law and promoted, but without such exaggerated importance that it devalues other laudable social goals?

I. THE NORMATIVE DEBATE ON BORDERS AND TERRITORIAL SOVEREIGNTY

It seemed inevitable that the question of regulatory authority in the online environment would end in conflict. In its infancy, as a largely unregulated space, a particular vision of the Internet emerged. It was one of freedom, liberty, and self-regulation.[10] Perhaps the imposition of off-line legal systems was inevitable, but not without resistance.

A. Outlining the Johnson-Post-Goldsmith Debate

Professors Johnson and Post set the initial parameters of the debate in their 1996 article, "Law and Borders - The Rise of Law in Cyberspace."[11] At the core of their argument is a vision of cyberspace as a distinct sphere, in which a discrete system of legal rules and regulatory processes should be permitted to evolve.[12] In advocating this result, their challenge is two-fold: First, to describe the separateness and singularity of cyberspace;[13] and second, to prove the propriety of self-regulation, largely to the exclusion of existing off-line legal systems grounded in territorially-based sovereignties.[14] The latter argument proceeds along concomitant lines, both drawn on their description of cyberspace as a distinct realm. As a practical matter, Johnson and Post challenge the practical feasibility of imposing external regulation on a borderless

---

10 See e.g., James Boyle, Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors, 66 U. Cin. L. Rev. 177, 177-79 (1997) (describing the "Internet Holy Trinity" of "digital libertarianism"); Margaret Jane Radin and R. Polk Wagner, The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace, 73 Chi.-Kent L. Rev. 1295, 1297 (1998) (describing "cyberlibertarians" and "anarcho-cyberlibertarians.").

11 See Johnson & Post, supra n. 3.

12 See e.g, id. at 1400-01 (concluding that Global electronic communications have created new spaces in which distinct rule sets will evolve. We can reconcile the new law created in this space with current territorially based legal systems by treating it as a distinct doctrine, applicable to a clearly demarcated sphere, created primarily by legitimate, self-regulatory processes, and entitled to appropriate deference--but also subject to limitations when it oversteps its appropriate sphere).

13 Id. at 1370-76, 1378-81.

14 Id. at 1387-91.

and boundary-destroying network.[15] Then, building on these infeasibility claims, they challenge the legitimacy of doing so.[16] This final assertion, which became of the focus of the authors' debate with Prof. Goldsmith, is described below.

Johnson and Post begin by acknowledging the primary importance of territorial borders to the existing system of determining legal rights and responsibilities, and accepting that this correlation makes sense in the off-line world.[17] Such validity, according to Johnson and Post, is based on the logical relationship between territorial borders and four related considerations: Power, legitimacy, effects, and notice.[18] The power to control a particular area of physical space, and the people and things located therein, "is a defining attribute of sovereignty and statehood."[19] This power rests on the singular ability of the sovereign to enforce the law within its borders.[20] The legitimacy of sovereign power is, in turn, premised on the "consent of the governed" - the idea that "persons within a geographically defined border are the ultimate source of law-making authority for activities within that border."[21] The exclusivity of sovereign power, to the exclusion of external forces, is rooted in the "relationship between physical proximity and the effects of any particular behavior," at least where there is no substantial overlap.[22] Finally, as a practical matter, territorial borders serve as signposts giving notice that a new regulatory regime now applies.[23]

The Internet, Johnson and Post claim, by its nature destroys the link between territorial borders and these validating principles.[24] Specifically, its decentralized architecture deprives territorially-based sovereigns of the power, or ability, to regulate online activity.[25] Likewise, claims of legitimacy based on the consent of the governed, and of exclusivity based on greater local effects, fail in a network of undifferentiated, simultaneous, and universal access.[26] Particularly problematic in this regard, the loss of these limiting principles results in overlapping and inconsistent regulation of the same activity, with significant spillover effect.[27] Moreover, in a network without geographical identifiers there is no notice of changing (and competing) regulatory regimes.[28] In the absence of these validating relationships between geographic borders and the space sought to be regulated, territorially-based sovereigns are deprived of their claim to

15 Id. at 1370-73.
16 Id. at 1374-76.
17 Id. at 1369-70.
18 Id.
19 Id. at 1369.
20 Id.
21 Id. at 1369-70
22 Id. at 1370.
23 Id.
24 Id. at 1370-76.
25 Id. at 1371-73.
26 Id. at 1375.
27 Id. at 1374.
28 Id. at 1375.

determine legal rights and responsibilities within that space.[29]

In retort, Professor Goldsmith criticizes the Johnson-Post arguments at several points.[30] On a macro level, he criticizes their limited view of sovereignty and over-reliance on the relationship between physical proximity and territorial effects.[31] Specifically, Goldsmith argues that "a nation's prerogative to control events within its territory entails the power to regulate the local effects of extraterritorial acts," including the harmful local effects of online activity.[32] The issue of enforcement power is challenged on three fronts: First, that Johnson and Post overstate the impossibility of regulation, mistaking ability for cost;[33] second, that they fail to recognize the deterrent effect of local enforcement, against end users and network components located within the territory, on extraterritorial actors;[34] and third, that they mistakenly equate valid regulation with some measure of near-perfect enforcement.[35] The problems of simultaneous, overlapping, and contradictory regulation of the same activity, and the spillover effects of these unilateral regimes, are, Goldsmith argues, likewise overstated.[36] As a practical matter, restrictions on jurisdiction and enforcement (byproducts of limited territorial sovereignty) mean that extraterritorial actors have little fear.[37] Moreover, Johnson and Post fail to articulate how the potential for simultaneous, overlapping, and contradictory regulation deprives an individual sovereign of the right to legitimately regulate on the basis of local effects.[38] Finally, the issue of notice is, Goldsmith argues, exaggerated, because content providers are on general notice that the data they provide might find its way into multiple jurisdictions, including those in which it is illegal.[39] In response, content providers may decide to condition access to data on the basis of geographic location.[40]

Narrowing his argument, Goldsmith identifies what he sees as a mistaken premise underlying Johnson and Post's assertion that territorial sovereigns have no authority to regulate the local effects of activities taking place outside their borders. Goldsmith argues that Johnson and Post mistakenly embrace a repudiated conception of choice-of-law

---

29 Id. at 1375-76.

30 In describing Professor Goldsmith's arguments, I refer to both his direct response to Professors Johnson and Post, see Goldsmith I, supra n. 3, and a related essay published in conjunction with the Indiana Journal of Global Legal Studies' symposium on "The Internet and the Sovereign State: The Role and Impact of Cyberspace on National and Global Governance," see also Goldsmith II, supra n. 3.

31 Goldsmith I, supra n. 3, at 1239-40; Goldsmith II, supra n. 3, at 476-77.

32 Goldsmith I, supra n. 3, at 1239.

33 Goldsmith II, supra n. 3, at 478-79.

34 Id. at 481-82.

35 Id. at 478-83.

36 Goldsmith I, supra n. 3, at 1340-42; Goldsmith II, supra n. 3, at 483-86, 487-90.

37 Goldsmith II, supra n. 3, at 488-89.

38 Goldsmith I, supra, n. 3, at 1240-42.

39 Id. at 1243-44.

40 Id.

principles grounded in the "belief in a unique governing law for all transnational activities;"[41] a notion that has "given way to the view that more than one jurisdiction can legitimately apply its law to the same transnational activity" and "the reality of overlapping jurisdictional authority."[42] In support of this view, Goldsmith first argues, as a practical matter, that it is equally feasible to apply this conception in cyberspace as it is in the offline environment, because various legal and technological tools - private legal ordering, the limits of enforcement jurisdiction, indirect regulation of extraterritorial activity, filtering and identification technology, and international cooperation - greatly reduce instances of true conflict.[43] In the resolution of these true conflicts, the problems, tools and solutions are no different in the online environment than in the off-line world; in other words, there is nothing special about cyberspace in this regard.[44]

At this point, Goldsmith is left to address Johnson and Post's claims that extraterritorial regulation is itself illegitimate, in part because the spillover effects of such regulation and the inability to provide effective notice in cyberspace make it so.[45] Goldsmith's response is a rather dismissive, "welcome to the modern world."[46] Extraterritorial regulation of local effects, and the spillover that results from that regulation, are now simply accepted.[47] The issue of notice is likewise dismissed rather easily; at most, it is reasonably foreseeable that data will be available to a multitude of jurisdictions with different regulatory standards, and the data supplier must choose how to limit access accordingly.[48]

Here, an otherwise useful discussion falters. Post is left to quarrel about functional identity,[49] as well as the consequence of transactional differences, in terms of scale and effect, on the principles of choice of law and prescriptive jurisdiction.[50] It is not that these questions do not matter, they are simply misplaced.

By conflating at the outset arguments of preference with those of validity, and questions of analytic jurisprudence with those of normative jurisprudence, Johnson, Post, and Goldsmith lose sight of the relationship between territorial sovereignty and the existence, sources, and validity of laws and legal systems, as distinguished from purposes, values, and virtues. This failure is rooted in the initial parameters of the debate - the offered dichotomy between descriptive and normative arguments; the very characterization of the latter arguments as exclusively normative; and the definition of valid sovereign power in terms of power, legitimacy, effects, and notice. It is in these

---

41 Id. at 1208.
42 Id.
43 Id. at 1212-32.
44 Id. at 1232-37.
45 Id. at 1239-42.
46 Id. at 1239.
47 Id. at 1239-42.
48 Id. at 1243-44.
49 Post, supra n. 3, at 1373-76.
50 Id. at 1376-84.

weaknesses that the debate fails.

B. Weaknesses in the Approach

Johnson-Post's vision of cyberspace, as a distinct sphere in which a discrete system of legal rules and regulatory processes should be permitted to evolve, stands in opposition to the dominant off-line model of legal regulation - territorial, sovereign-based legal systems - sought to be imposed on the online environment. It is this advocacy for self-regulation, rather than external controls promulgated, adjudicated, and enforced outside the "distinct sphere" of cyberspace, that motivates and directs the Johnson and Post argument.[51] In support of their position, Johnson and Post make essentially a two-tiered argument. First, as a descriptive matter, self-regulation is preferable simply because it works better.[52] Not only is self-regulation desirable in its own right, because it has proven well-suited to the online environment (architecturally, as a matter of community, and so on), but even more so because the alternative - the imposition of external, territorially-based legal regimes - is infeasible, ineffective, and fundamentally damaging to the online environment. Second, as a "normative" matter, self-regulation is preferable because, according to Johnson and Post, territorially-based sovereigns lack valid authority to regulate outside their physical borders.[53] Yet the Internet is architected in such a way as to practically necessitate the extraterritorial exercise of regulatory power. It is in this second argument, stepping beyond preference and perceived superiority, to the broader claims of authority and validity, that the problems surface.

It is helpful to begin, as Johnson and Post do, with the idea of sovereignty and territorially-based systems of law - the dominant model of off-line regulatory power. Their claim of authority is grounded in claims of societal sovereignty which extend to boundaries of land and to groups of people within those boundaries.[54] Each sovereign maintains the existence of an identifiable legal system, comprised of valid laws. That system of laws is arguably applicable, as the claim of sovereignty would suggest, to acts occurring or having an effect within a particular territory, to an identifiable community of people, and, in certain circumstances, to those with whom members of the community interact. Generally, a particular system of laws reflects the customs, social practices, and moral ideals of that community, or its most powerful subset.[55] The law is generally

---

51 See Johnson & Post, supra n. 13, and accompanying text (arguing that "Global electronic communications have created new spaces in which distinct rule sets will evolve.").

52 See Johnson & Post, supra n. 16, and accompanying text (challenging the practical feasibility of imposing external regulation on the network).

53 See Johnson & Post, supra n. 25, at 1371-76, and accompanying text (arguing that the Internet destroys the link between borders and the validating principles of territorial sovereignty).

54 See e.g., Joseph Raz, The Concept of a Legal System: An Introduction to the Theory of Legal System 6-18 (2d Ed. Oxford University Press 1980, 1990) (discussing and commenting on various theories of sovereignty, including that of Bentham, Austin and Kelsen).

55 This rather simplistic statement admittedly ignores contentious questions regarding the existence and identity of law as law, as well as its validity. Legal positivism, the thesis of legal philosophy with which Joseph Raz is associated, views the existence, content and

created, modified and applied by institutions of the sovereign, and obedience to it is ultimately guaranteed by the use of force.[56]

With the emergence of a pervasive, resource-rich online environment, these dominant regulatory powers have rather predictably attempted to impose their legal regimes.[57] The validity of such imposition is both premised on the claim of sovereignty and presumably limited by it. Thus, the sovereign may claim the right to regulate the online activity of persons within its territory, and even its citizens when abroad.[58] These claims are among the least contentious, but the claims of sovereignty are not so narrow. For instance, online activities originating outside the territory but having an effect within the territory, on members of the society, or on the society itself, are potentially subject to the claims of the sovereign.[59]

With this description in hand, Johnson and Post's normative argument - that the regulation of cyberspace by territorially-based sovereigns constitutes the invalid exercise of extraterritorial authority[60] - can be understood as conflating what are in fact two discrete, if related attacks. The first builds on a particular descriptive narrative of cyberspace as a distinct sphere existing outside any territorial border, arguing that

---

validity of law as a matter of social fact, rather than a matter of moral content. See e.g., Stanford Encyclopedia of Philosophy: Legal Positivism, http://plato.stanford.edu/entries/legal-positivism/#4 (last accessed Apr. 3, 2005). Natural law theorists, on the other hand, insist on an essential connection between law and morality. Id.

56 See Raz, supra n. 54, at 3 (stating in pertinent part that the three most general and important features of the law are that it is normative, institutionalized, and coercive. It is normative in that it serves, and is meant to serve, as a guide for human behavior. It is institutionalized in that its application and modification are to a large extent performed or regulated by institutions. It is coercive in that obedience to it, and its application, are internally guaranteed, ultimately, by the use of force).

57 See e.g. Paul Schiff Berman, The Globalization of Jurisdiction, 151 U. Pa. L. Rev. 311, 315-16 (2002) (describing the movement of nation-states to regulate "almost every conceivable online activity.").

58 See e.g. id. at 317.

59 See e.g. id. (arguing that "these assertions of national authority have raised many of the legal conundrums regarding nation-state sovereignty, territorial borders, and legal jurisdiction that Johnson and Post predicted. " For example, if a person posts content online that is legal where it was posted but is illegal in some place where it is viewed, can that person be subject to suit in the far-off location? Is online activity sufficient to make one "present" in a jurisdiction for tax purposes? Is a patchwork of national copyright laws feasible given the ability to transfer digital information around the globe instantaneously? How might national rules regarding the investigation and definition of criminal activity complicate efforts to combat international computer crime? Should the law of trademarks, which historically has permitted two firms to retain the same name as long as they operated in different geographical areas, be expanded to provide an international cause of action regarding the ownership of an easily identifiable domain name? And, if so, should such a system be enforced by national courts (and in which country) or by an international body (and how should such a body be constituted)? And on and on).

60 See Johnson & Post, supra n. 3, at 1370-76.

territorially-based sovereigns cannot subsume authority over this separate space as if it were within their borders.[61] The second is premised on a specific conception of limited extraterritorial regulation, arguing that territorially-based sovereigns cannot validly regulate activities within cyberspace, even those having local effects, because most originate outside their borders - either within cyberspace or within the territory of another - and the effects of such activity are felt simultaneously throughout the network.[62] Both arguments are troublesome.

The first argument is captured in the asserted validating principles of power and legitimacy,[63] but there are at least two problems with this approach. As a practical matter, this argument relies too heavily on a literal separateness of cyberspace and is thus susceptible to rather simple competing arguments as to existing capabilities, technological advancement and choice.[64] Moreover, it reflects a problematic view of the network as divorced from its ends, which exist in particular territories.[65] On a more theoretical level, what are cast as normative arguments are in fact either analytical in nature[66] and overreaching, or hyper-normative[67] and thus unsupported in the existing

---

61 See e.g. id. at 1370 (describing the challenge of the Internet to territorially-based sovereign authority as the rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behavior; (2) the effects of online behavior on individuals or things; (3) the legitimacy of a local sovereign's efforts to regulate global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply. The Net thus radically subverts the system of rule-making based on borders between physical spaces... Id. at 1376 (concluding because events on the Net occur everywhere but nowhere in particular, are engaged in by online personae who are both "real" (possessing reputations, able to perform services, and deploy intellectual assets) and "intangible" (not necessarily or traceably tied to any particular person in the physical sense), and concern "things" (messages, databases, standing relationships) that are not necessarily separated from one another by any physical boundaries, no physical jurisdiction has a more compelling claim than any other to subject these events exclusively to its laws).

62 See e.g. id. at 1375 (describing the effects of online activity as being felt simultaneously throughout the network, "everywhere [and] nowhere in particular"); Id. at 1376 (arguing that "events on the Net occur everywhere but nowhere in particular.").

63 Id. at 1371-76.

64 Goldsmith II, supra n. 3, at 478-79, 481-82 (articulating these arguments). See also infra n. 77 (describing the Internet architecture as a choice, not a given).

65 See infra n. 78-83 and referenced text (describing the architecture of the Internet).

66 See generally Johnson & Post, supra n. 3 (Johnson and Post begin with the idea of sovereignty, describing it in terms of statehood and the power to control of a particular area of physical space, and the people and things located therein. From this description, they derive a limiting principle that correlates the validity of regulation with the ability to enforce. Although announced as a normative assertion, it seems clearly an analytic conception); see also Kenneth Einar Himma, The Internet Encyclopedia of Philosophy: Philosophy of Law, http://www.iep.utm.edu/l/law-phil.htm (last accessed June 26, 2006) (stating that analytic jurisprudence is concerned with what law is, while normative jurisprudence considers what law ought to be. Thus, analytic jurisprudence asks: What is law? What is a legal system? What is the relationship between law and morality? Id. Normative jurisprudence, on the other

system. As such, these attacks on the sovereign as sovereign are rather easily dismissed.

The second argument rests on the asserted validating principle of effects, which links the exclusivity of sovereign authority to a perceived relational connection between effects and physical proximity.[68] This claim may be interpreted (since Johnson and Post's intent here is unclear) in either of two ways. On one hand, this might require the conception of cyberspace as a "territory" separate from physical space, describing online activities as originating and existing solely within the online world, and regulation by off-line sovereigns as invalid extraterritorial assertions of authority.[69] Viewed this way, the argument suffers from the same difficulties described above - it is overly reliant on a particular descriptive narrative of cyberspace, and requires that we divorce the network from its territorially-based components. On the other hand, the argument can be interpreted as little more than a restatement of traditional conflicts arising from transnational activities and effects, or common resources.[70] From this perspective, the argument appears to ignore that many assertions of extraterritorial authority have been accepted in the off-line world. Areas of conflict - disputed territory, cross-border effects, common resources such as the oceans and outer space - have been resolved on a macro level, sovereign-to-sovereign, by force, negotiation, treaty, international organization, and the like.[71] Why should the Internet be any different?

It is on this axis, and these weaknesses, that the Johnson and Post argument turns. What began as an argument of preference, that the Internet should be different,[72] was oversold. It became an argument of existence, validity, and legal authority,[73] all of which hinged on acceptance of the Internet as necessarily different in significant ways, significant enough to undermine the entire foundation of an existing legal system based on territorial sovereignty. When the force of this argument was lost because it demanded

---

hand, asks: What is the proper function of law? Is there a duty to obey the law? What is the rule of law and what is its value? Analytic jurisprudence is also to be differentiated from theories of law grounded in history, political theory, or sociology); see also Raz, supra n. 54, at 15 (summarizing Austin's position that the power requirement - that a sovereign be able to enforce its laws - draws from the work of legal positivist John Austin, who (in greatly simplified terms) defined a law as a general command of a sovereign addressed those likely to suffer the prescribed sanction. Laws were required to be part of a legal system, and that system was required as a measure of validity to be on the whole effective. Leveraging this analytic statement about law as law, Johnson and Post argue that if the authority of law is derived from sovereign power, so are its limits).

67 For instance, perhaps legal authority ought to be premised on the consent of the governed, see Johnson & Post, supra n. 22, 27 and referenced text, but that aspiration cannot serve as a defining and limiting principle. To argue otherwise is to suggest the illegitimacy of all non-democratic regulatory schemes, a seemingly broader claim than Johnson and Post intend.

68 Id. at 1369, 1375.

69 Id. at 1375.

70 Id. at 1208-42.

71 Id.

72 Id. at 1387-91.

73 Id. at 1375-76.

too much, Johnson and Post were left to argue either the extreme, or the ordinary and predictable.

By overreaching, Johnson and Post allowed the debate to get away from them. What should be a contest of choices about a unique sphere, should we recognize and protect the exceptionalities of cyberspace as it currently exists? Will self-regulation better serve that goal than externally imposed legal regimes? How may the two best coexist? - becomes a fairly pedestrian argument about sovereign power and its limits. Rather than discussing what law ought to be, so as to best serve its purposes, values, and virtues, Johnson and Post are left with the monumental task of describing cyberspace in such a way as to support a level of exceptionalism that changes the very concept of what law is. True, they attempt to characterize this as a purely normative argument, but these hallow distinctions only make Professor Goldsmith's job easier.

II. REFRAMING THE DEBATE

Johnson and Post's mistake, I believe, was their very focus on sovereignty. The harms Johnson and Post identify are harms to the individual, which are in turn seen as harming cyberspace itself. But in proving these harms, why seek to nullify an entire system by focusing on the individual's validating relationship with existing sovereigns?[74] Why not the individual as autonomous actor? Might not individual harms be addressed through established conceptions of normative jurisprudence serving the purposes, values, and virtues of law? In the following section, I seek to reorient the analysis and approach the issue from a slightly different perspective, focusing instead on conformity to the rule of law as a negative value - limiting law in its form and application - so as to restrain arbitrary power, protect personal freedom, and promote human dignity.

A. Preliminary Points of Law, Legal Systems, and Internet Architecture

As the preceding discussion suggests, questions of normative jurisprudence, particularly as an abstract inquiry, often elude or subsume questions of the nature of law and legal systems - their existence, sources, content, and validity - just as they incorporate assumptions as to that nature. It is much more difficult to escape these concerns in the context of a specific legal construct, as here particularly, where the criteria of that construct (the online environment) remain largely unfamiliar and contentious. Thus, it is better to acknowledge a few presumptions - grounded in specifics but implying certain views of abstract analytic jurisprudence - define their borders, and move on.

---

[74] One might argue that individuals possess an online legal identity separate from their off-line persona. This online persona would have both a validating relationship to whatever discrete legal authority develops in cyberspace, and a “foreign citizen” relationship with existing territorial-based sovereignties. This would allow the “citizens” of cyberspace to develop their own rules and analysis for resolving areas of conflict. The difficulties of such an approach are, however, innumerable.

We begin, first, by presupposing the existence and validity of territorially- and sovereignty-based systems of law as law.[75] With the normative question thus unhinged, we focus on the relationship between the individual and the purposes and values of law, rather than as a validating mechanism of sovereign power.

The descriptive element is likewise treated circumspectly, because it plays a much different role in the analysis. Johnson and Post must necessarily define cyberspace as an area fundamentally distinct from physical territory, so as to create the comparative distinction from territorially-based legal systems. My goal here is more limited; to describe functional differences in the pervasive (rather than distinct) online environment and areas of conflict against which the normative concept is applied.

As currently structured[76] the Internet presents a rather basic challenge to territorially-based regulatory regimes. Here, it is helpful to envision the structure of the network in greatly simplified terms, as consisting of three levels.[77] The physical level is comprised of

---

[75] It should be noted that this article intentionally does not employ the term "cyberlaw." That term is more one of debate than definition. While it acknowledges the Internet as a developing, unregulated resource and concedes the effect of law, in its broadest sense, on the distribution of power over and within that resource, it leaves unsettled, at the very least, whether "cyberlaw" is: an internal, "indigenous" regime or an imposed, external regime; a legal regime or a technological, code-based regime; and a regime derived from territorially-based sovereigns or from international regulation and enforcement - convenient dichotomies that brush just the surface of that debate.

[76] As an organic technology, the Internet is ever-changing. It is a structure of choices, architected by network design principles, nearly all of which may be altered. See Lawrence Lessig, Code and Other Laws of Cyberspace 217 (Basic Books 1999) (stating that "cyberspace... has different architectures.... An extraordinary amount of control can be built into the environment that people know there. What data can be collected, what anonymity is possible, what access is granted, what speech will be heard--all these are choices, not 'facts.' All these are designed, not found."). Please note that I deal here with the Internet as it exists at a moment in time. But this does not necessarily undermine the analysis; indeed, my argument is that the value of conformity to the rule of law should inform these choices, see infra section III.

[77] See Lawrence Lessig, The Architecture of Innovation, 51 Duke L.J. 1783, 1786, 1788-90 (2002) (building on the communications-systems work of Yochai Benkler). As issues of architecture and data are not the intended focus of the paper, this discussion is sharply limited. For those more interested in these subjects, I would recommend, in addition to the footnoted materials, Timothy Wu, Application-Centered Internet Analysis, 85 Va. L. Rev. 1163, 1189-93 (1999) (discussing the importance of a layered network architecture and end-to-end design, as critical to any legal analysis of the internet). For a more technical examination of how this model works, it may be helpful to think of this three-layered system as a simplified version of the Open System Interconnection, or OSI Model which is used in teaching computer science. See The 7 Layers of the OSI Model, http://www.webopedia.com/quick_ref/OSI_ Layers.asp (last accessed Mar. 5, 2005) (explaining the OSI Model via a table while also providing a graphic to show the path that data packets take from one computer to the next). Benkler's simplified version appears to be based upon layers one, three, and seven of the OSI Model.

material objects - wires, computers, and wires linking computers.[78] The logical level consists of open protocols governing the exchange of data across the network.[79] The content level is the digital data itself, which is easy to access, copy, distribute, and exchange.[80] Coincident with this vertical conception, the Internet is architected according to end-to-end design principles: The intelligence rests at the ends; the ends are connected by a simple, decentralized network.[81] This simplicity arises from open protocols and non-discriminatory, neutral data transfer.[82]

As a result of these architecting choices, regulations aimed at the middle of the network, away from the ends, are met largely with technical indifference.[83] The network is built to move data indiscriminately, without judgment.[84] This necessarily pushes regulation toward the end user data recipient, where enforcement can be grossly inefficient. Yet, attempts to move enforcement upstream, to bigger pipes and switches handling greater amounts of data, have proven clumsy, damaging to permissible uses, mostly ineffective, and strikingly undemocratic.[85] It is thus extremely difficult for

---

78 See Lessig, supra n. 77, at 1788-89.

79 Id. at 1789.

80 Id. at 1789-90.

81 Id. at 1789 (stating that "the core of the Internet's design is an ideal called 'end-to-end' (e2e)... [which contemplates networks designed] so that intelligence rests in the ends, and the network itself remains simple.").

82 Id. ("The network [is] simple, or 'stupid,' in David Isenberg's sense, and the consequence of stupidity, at least among computers, is the inability to discriminate" on the basis of data content).

83 While this may seem to be an overstatement, consider the technical basis for the "end-to-end" design theory. The basic unit of network communication is the packet. Think of a packet like a train with many different cars or sections. The front sections of a packet, the "header," contain addressing information. The header simply tells the network "this is where I'm going, and this is where I came from." It is the job of the end of the network - the computer - to reach out and claim the packet should the IP address of the computer match that of the packet's destination address. Following the header is the data itself - this could be a tiny piece of an e-mail, broken down into 1's and 0's. Finally, the trailer brings up the rear of our packet train and contains components to assist with error checking to make sure that the packet does not need to be resent by the sender. The network really is simple in that it simply moves the packets based upon the packet's instructions. The computers at the ends of the network perform the "smart task of reassembling and interpreting the packets. Any discrimination or complexity built into Lessig's "logical layer" is only meant to assist with the addressing function of the packet (i.e. "switching" among larger interconnected networks). See Microsoft Press, Networking Essentials 193-97 (2d ed. 1997).

84 See Lessig, supra n. 76, at 1789.

85 It is certainly not the case that such ham-handed regulation is impossible. See e.g. Joseph Kahn, "China Has World's Tightest Internet Censorship, Study Finds," New York Times (Dec. 4, 2002) (reporting that China was able to "block up to 50,000 sites at some point in the six-month period" because the Internet, unlike telephones for instance, "has common checkpoints. All traffic passes through routers that make up the telecommunications backbone here. China blocks all access to many sites, and it has begun selectively filtering content in

regulators to restrict the availability of objectionable data without pursuing the source - i.e., the intelligent ends of the network from which data is available. These sources often supply an exponential number of users, multiplying the net effect of successful enforcement.

From this description, the complexities of applying a territorially-based regulatory regime to the online environment become apparent. At one end of the network, that physically located within a sovereign's territory, the sheer number of data recipients makes regulation costly and inefficient. In the middle, the network is decentralized and indiscriminate,[86] and the digital data itself eludes content-based distinctions,[87] making it nearly impossible to efficiently regulate data flow, much less to superimpose concepts like knowledge and intent. At the other end, a smaller number of data suppliers are providing objectionable content. Although these data suppliers represent an obvious target for regulators, they are often scattered throughout the world in a multitude of sovereign territories. Still, territorial regulators may claim that the online activities of extra-territorial data suppliers have a perceived effect within the territory, on members of the society or on the society itself.

Apart from more directed efforts, many suppliers merely provide a static platform of data, such as public web sites[88] and bulletin boards,[89] accessible without differentiation. Even where selective access is desired, distinctions based on geographic location and similar standards are generally ineffective. It is quite simple for both data recipients and suppliers to remain anonymous or pseudonymous, or to take on false and misleading identities.[90] It is therefore difficult (and often undesirable) for data suppliers to exercise

---

real time--even as viewers seek access to it--and deleting individual links or Web pages that it finds offensive.").

86 See supra n. 84-85 and referenced text.

87 The decentralized nature of the network makes it difficult to exercise external, network-based control over the data once it is released. See Reno v. ACLU, 521 U.S. 844, 853 (1997) (quoting lower court findings, 929 F.Supp. 824, 844 (finding no. 86)) ("Once a provider posts its content on the Internet, it cannot prevent that content from entering any community."). Of course, the absence of external, network-based control should be distinguished from content management tools existing within the data itself.

88 A Web Site is described as "the entire collection of web pages and other information (such as images, sound, and video files, etc.) that are made available through what appears to users as a single web server." Matisse Enzer, Glossary of Internet Terms: "Web Site," http:// www.matisse.net/files/glossary.htmlindex (last accessed Apr. 4, 2005).

89 Id. (stating that a Bulletin Board System is described as a computerized meeting and announcement system that allows people to carry on discussions, upload and download files, and make announcements without the people being connected to the computer at the same time. In the early 1990's there were many thousands (millions?) of BBS's around the world, most are very small, running on a single IBM clone PC with 1 or 2 phone lines. Some are very large and the line between a BBS and a system like AOL gets crossed at some point, but it is not clearly drawn).

90 See A. Michael Froomkin, Anonymity and Its Enmities, J. Online L. (1995) http://www.wm.edu/law/publications/jol/95_96/froomkin.html (last accessed Dec. 19, 2004)

discretion, even where distribution is more active and deliberate, as with email.[91] This inability and/or refusal to limit access to, and distribution of, data on a territorial basis, so as to comply with the various territorially-based regulatory regimes and eliminate the perceived deleterious effects of objectionable data, creates the areas of conflict with which I am concerned.

To this point I have described some of the principles underlying the dominant legal systems and presumed their abstract validity. I have also generally described the architecture of the Internet, and the problems that that architecture poses for these legal systems. I now ask the normative question: Does the extension of these systems into the online environment serve the most basic principles, purposes, and values of law?

B. Raz's Conception of the Rule of Law and Its Virtue

Because the focus of this article is narrow, constructive discussion requires the setting of boundaries that are broad enough to be useful, yet reasonably restrictive. I have chosen to cabin my analysis through the adoption of a rather specific and formalistic conception of the rule of law; that put forward by legal philosopher Joseph Raz.[92] This conception serves as a steady framework, paradoxically allowing for greater freedom in assessing whether the governance of cyberspace by traditional laws imposed by territorially-based sovereigns conforms to the rule of law. It is important, therefore, to clarify precisely what the rule of law is, and is not, for purposes of this discussion. Even

(observing that "[b]asically, anything you can do with words and pictures, you can do anonymously on the Internet.") For an interesting early discussion of anonymous online speech see Lee Tien, Who's Afraid of Anonymous Speech? McIntyre and the Internet, 75 Or. L. Rev. 117 (1996). The opportunity for anonymity is a product of both the data and the network. Because Internet communications are digital, "the only identifying marks they carry are information inserted by the sender, the sender's software, or by any intermediaries who may have relayed the message while it was in transit." See Froomkin, supra n. 90, at 415. In its current incarnation, identification by the decentralized network that carries (or "relays") your message can be largely avoided. See e.g., Lessig, supra n. 76, at 26-28, 217. Thus, anonymous online speech and interaction remains a viable option, made available by the network architecture, technologies of anonymity, and user choice; see also Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules Through Technology, 76 Tex. L. Rev. 553, 574-75 (1998); Mathius Strasser, Beyond Napster: How the Law Might Respond to a Changing Internet Architecture, 28 N. Ky. L. Rev. 660, 707-08 (2001) (describing peer-to-peer architecture, Freenet, and anonymous nodes).

91 See Enzer, supra n. 88 (describing e-mail as "[m]essages, usually text, sent from one person to another via computer. E-mail can also be sent automatically to a large number of addresses.").

92 Joseph Raz is Professor of the Philosophy of Law at Oxford University, Fellow of Balliol College, and Visiting Professor at Columbia University School of Law and a member of the Department of Philosophy. He is a Fellow of the British Academy and a Foreign Honorary Member of the American Academy of Arts and Sciences. See Joseph Raz, Biographical Information, http:// users.ox.ac.uk/~raz/index_files/page0004.htm (last visited Mar. 19, 2006).

at the most basic level, the rule of law is a complex and difficult idea.[93] A summary of that concept, although intended to make it more accessible, is thus necessarily incomplete. Nevertheless, because the precise contours of the rule of law are not the focus of this article, I will undertake to do so here, pausing briefly to explore some of the more important points of disagreement and their effect, if any, on my analysis.

In his 1977 article, "The Rule of Law and Its Virtue," Raz sets forth a defining formalistic conception of the rule of law.[94] The article begins by embracing a formulation of the ideal of the rule of law set forth by F.A. Hayek:

> [S]tripped of all technicalities [the rule of law] means that government in all its actions is bound by rules fixed and announced beforehand - rules which make it possible to foresee with fair certainty how the authority will use its coercive powers in given circumstances, and to plan one's individual affairs on the basis of this knowledge.[95]

Drawing on this formulation, Raz asserts that, in its most literal sense, the rule of law comprises two broad requirements: "(1) that people should be ruled by the law and obey it, and (2) that the law should be such that people will be able to be guided by it."[96] Placing greater emphasis on the latter, and in Raz's view the more important and complex of these constraints,[97] the "basic intuition" of Raz's formalistic conception of the rule of law is that "the law must be capable of guiding the behavior of its subjects."[98] From this foundation, Raz then derives eight broad principles incumbent in the ideal of the rule of law.[99]

The first three of these principles are enabling - demanding that the law conform to certain standards that facilitate the law's effective guidance of individual action:[100]

---

93 See Andrei Marmor, The Rule of Law and Its Limits, 23 USC Law and Public Policy Research Paper No. 03-16, 1 (Apr. 2003), http:// ssrn.com/abstract=424613 (calling the rule of law a "complicated idea" and noting that "the various ideas associated with the rule of law are often conflicting and not infrequently rather confused.").

94 See Raz, supra n. 2.

95 F.A. Hayek, The Road to Serfdom 54 (Routledge Press 1944).

96 See Raz, supra n. 2, at 213.

97 See generally id. at 233-49 (discussing the obligation to obey the law). Indeed, it is unclear whether Raz accepts the first broad requirement - that people should be ruled by the law and obey it - at all.

98 Id. at 214.

99 Each of these eight principles "directly concern[s] the system and method of government in matters directly relevant to the rule of law." Id. at 218. As Raz himself realizes, "[t]his list [of eight principles] is very incomplete." Id. Indeed, the multitude of systems and "the particular circumstances of different societies" imply a host of principles to be derived from the rule of law; "[t]here is little point in trying to enumerate them all." Id. at 214. These eight principles merely embody "some of the more important ones." Id.

100 Id. at 214.

Laws should be prospective,[101] open and adequately publicized,[102] and their meaning clear.[103]

Laws should be reasonably stable and constant, without frequent change.[104] This promotes knowledge of what the law is,[105] the ability to make short-term decisions, and the capacity for long-term planning.[106]

There should be a stable framework of general rules that guide the making of particular laws and legal orders.[107] These general rules should both confer the authority to make such orders, and, at the same time, impose duties and restrictions on power-holders in the exercise of that authority.[108]

To these three principles, I would add two more that enjoy wide support from both those who agree with Raz's views and his critics.[109] First, there should be no contradictory laws, for "if the [law] prescribes one thing and at the same time its contradiction, people cannot follow it."[110] Second, there should be no laws that, although comprehensible and consistent, are in practice impossible to follow.[111] Both of these principles serve Raz's "basic intuition" of the rule of law - that the law should be capable of guiding the behavior of its subjects[112] - and fit neatly with the enabling principles that he identifies.

---

101 Id. (stating that "one cannot be guided by a retroactive law.").

102 Id. (arguing that "if [law] is to guide people they must be able to find out what it is.").

103 Id. (stating that "an ambiguous, vague, obscure, or imprecise law is likely to mislead or confuse at least some of those who desire to be guided by it.").

104 Id.

105 Id. at 214-15 (pointing out that [i]f [laws] are frequently changed people will find it difficult to find out what the law is at any given moment and will be constantly in fear that the law has been changed since they last learnt what it was."). This is, of course, closely tied to the requirement of, and degree to which, laws are open and adequately publicized. A lack of accessibility may be offset somewhat by greater stability; once the individual learns what the law is, it is unlikely to change. On the other hand, if law is both inaccessible and unstable, then the challenge to the rule of law is exponentially greater.

106 Id. at 214-15 (arguing that "more important still is the fact that people need to know the law not only for short-term decisions... but also for long-term planning"); Id. at 215 (for example knowledge of at least the general outlines and sometimes even of the details of tax law and company law are often important for business plans which will bear fruit only years later. Stability is essential if people are to be guided by law in their long-term decisions).

107 Id.

108 Id. at 216.

109 Id. at 218 (noting that his list of principles "is very incomplete" and that '[o]ther principles could be mentioned"). Raz certainly remained open to the addition of other principles incumbent in the ideal of the rule of law.

110 See Marmor, supra n. 93, at 7.

111 Id. at 7-8.

112 See Raz, supra n. 2, at 214.

The remaining five principles are "designed to ensure that the legal machinery of enforcing the law should not deprive it of its ability to guide [individual action] through distorted enforcement and that [the law] shall be capable of supervising conformity to the rule of law and provide effective remedies in cases of deviation from it":[113]

The judiciary should be independent, for "it is futile to guide one's actions on the basis of the law if when the matter comes to adjudication the courts will not apply the law and will act for some other reason."[114]

Certain procedural safeguards should be observed - open and fair hearings, and absence of bias - as they are "essential for the correct application of the law and thus . . . to its ability to guide action."[115] Courts should have review powers to ensure, at the very least, conformity to the rule of law.[116] Courts should be easily accessible.[117] Impediments, such as long delays and excessive costs, serve only to "frustrate one's ability effectively to guide oneself by the law."[118] The discretionary powers of law enforcement should not be permitted to pervert application of the law.[119] Finally, it should be well-noted that these principles, although derived from the rule of law, are not intended to stand on their own.[120] Rather, they are to be interpreted against the basic idea of the rule of law, that the law should be capable of guiding the behavior of its subjects.[121]

Having thus outlined Raz's conception of the rule of law and some of the more important principles that may be derived from that conception, it is important to pause at this point to emphasize certain attributes potentially ascribed to law and a legal system which are not within Raz's ideal. Raz argues that many legal theorists - as well as politicians, social commentators, and the like - have made "promiscuous use" of the term "the rule of law."[122] It has evolved into a sort of central tenet, or a system within itself,

---

113 Id. at 218.

114 Id. at 216-17 (stating that since the court's judgment establishes conclusively what is the law in the case before it, the litigants can be guided by law only if the judges apply the law correctly. Otherwise people will only be able to be guided by their guesses as to what the courts are likely to do - but their guesses will not be based on the law but on other considerations). Id. at 217 (stating that the rules concerning the independence of the judiciary - the method of appointing judges, their security of tenure, the way of fixing their salaries, and other considerations of service - are designed to guarantee that they will be free from extraneous pressures and independent of all authority save that of the law. They are, therefore, essential for the preservation of the rule of law).

115 Id.

116 Id.

117 Id. ("given the central position of the courts in ensuring the rule of law... it is obvious that their accessibility is of paramount importance.").

118 Id.

119 Id. at 218 (suggesting that such perversion might arise through selective prosecution or the uneven allocation of resources to certain crimes or classes of criminals).

120 Id. at 218.

121 Id.

122 Id. at 211.

under and within which all of our most basic principles must fall.[123] So perceived, the rule of law requires certain processes (democracy), certain content (some conception of basic human rights), and a certain outcome (justice).[124] Raz rejects this view and these requirements,[125] finding value in the rule of law without these added burdens.

Although I personally find Raz's conception of the rule of law to be more useful and compelling, and what may be termed broader conceptions less so, a defense of that position is beyond the scope this article. Rather, I have chosen Raz as an analytical tool precisely because his conception of the rule of law is a narrow and formalistic one. Raz captures the common ground, such as it is, without the more grandiose ideals. On this ground alone, the rule of law fails in cyberspace. We need not go so far as to test the governance of cyberspace by traditional laws against the ideals of democracy, justice, and basic human rights. Even without these requirements, the rule of law, as conceived by Raz, has great value, and it is enough to say that the governance of cyberspace by traditional law fails this slender reed.

Raz identifies at least three important values to the individual that are served by conformity to the rule of law. First, it restrains many of the most injurious aspects of arbitrary power: The government is prevented from arbitrarily "changing the law retroactively or abruptly or secretly whenever this suits its purposes;" public officials are greatly restricted in the "arbitrary use of power for personal gain, out of vengeance or favouritism."[126] Second, it protects personal freedom, in the sense that such freedom lies in the "effective ability to choose between as many options as possible."[127] Conformity to

---

123 Id.

124 Id.

125 See Raz, supra n. 2, at 211 (arguing that "the rule of law is just one of the virtues which a legal system may possess and by which it is to be judged. It is not to be confused with democracy, justice, equality (before the law or otherwise), human rights of any kind or respect for persons or for the dignity of man."); Id. (buttressing this point by discussing that a non-democratic legal system, based on the denial of human rights, on extensive poverty, on racial segregation, sexual inequalities, and religious persecution may, in principle, conform to the requirements of the rule of law better than any of the legal systems of the more enlightened Western democracies. This does not mean that it will be better than those Western democracies. It will be an immeasurably worse legal system, but it will excel in one respect: in its conformity to the rule of law); see also id. at 214 ("[i]t is evident that this conception of the rule of law is a formal one. It says nothing about how the law is to be made: by tyrants, democratic majorities, or any other way. It says nothing about fundamental rights, about equality, or justice."). Raz is particularly careful to make this point when discussing the idea that the making of particular laws should be guided by open, stable, clear, and general rules. See id. 215 ([t]here is "a belief that the rule of law is particularly relevant to the protection of equality and that equality is related to the generality of law. The last belief is, as has often been noted before, mistaken. Racial, religious, and all manner of discrimination are not only compatible but often institutionalized by general rules.").

126 Id. at 219-20.

127 Id. at 220 (emphasizing that the personal freedom of effective choice that is protected by the rule of law differs from political freedom). Id. at 220-21 (discussing that "political freedom

the rule of law promotes "stable, secure frameworks for one's life and actions," and such predictability allows the individual to fix long-term goals and effectively direct one's life toward those goals.[128]

The third, and most important value recognizes that "observance of the rule of law is necessary if the law is to respect human dignity":

Respecting human dignity entails treating humans as persons capable of planning and plotting their future. Thus, respecting people's dignity includes respecting their autonomy, their right to control their future. . . . The law can violate people's dignity in many ways. Observing the rule of law by no means guarantees that such violations do not occur. But it is clear that deliberate disregard for the rule of law violates human dignity.[129]

Absent the rule of law, there may be uncertainty or frustrated expectations.[130] Uncertainty arises when "the law does not enable people to foresee future deployments or to form definite expectations (as in cases of vagueness and most cases of wide discretion)."[131] Expectations are frustrated when "the appearance of stability and certainty which encourages people to rely and plan on the basis of existing law is shattered by retroactive law-making or by preventing proper law-enforcement, etc."[132] Thus, this third value is illuminated by the first and second, for "[t]he evils of uncertainty are in providing opportunities for arbitrary power and restricting people's ability to plan for their future."[133]

Beyond these values to the individual, Raz sees conformity to the rule of law as an inherent value of law itself, serving a functional purpose.[134] Conformity to the rule of law is, Raz argues, "essential for securing whatever purposes the law is designed to achieve."[135]

---

consists of: (1) the prohibition of certain forms of behavior which interfere with personal freedom and (2) the limits imposed on the powers of public authorities in order to minimize interference with personal freedom.... The rule of law may be yet another mode of protecting personal freedom. But it has no bearing on the existence of spheres of activity free from governmental interference and is compatible with gross violations of human rights.").

128 Id. at 220.

129 Id. at 221.

130 Id. at 222.

131 Id. at 222.

132 Id.

133 Id.

134 Id. at 226.

135 Id. at 224 (distinguishing between direct and indirect purposes of the law, the author gives the following example: "[A] law prohibiting racial discrimination in government employment has as its direct purpose the establishment of racial equality in the hiring, promotion, and conditions of service of government employees (since discriminatory action is a breach of the law). Its indirect purposes may well be to improve race relations in the country in general, prevent a threat of strike by some trade unions, or halt the decline in popularity of the

These [purposes] are achieved by conformity with the law which is [in turn] secured . . . by people taking note of the law and guiding themselves accordingly. Therefore, if the direct purposes of the law are not to be frustrated it must be capable of guiding human behavior, and the more it conforms to the principles of the rule of law the better it can do so."[136]

This functional value is, in Raz's view, the essence of the rule of law in relation to law itself.[137]

As with the content of the rule of law, Raz's conception of the rule of law as an inherent, yet merely functional virtue of the law is distinct in its limitations. Specifically, Raz rejects the idea that there is a necessary connection between the law - and the rule of law - and morality: "the rule of law is an inherent virtue of the law, but not a moral virtue as such."[138] The metaphor Raz employs to make this point is helpful: Although being sharp is an important inherent characteristic of a good knife - i.e., a characteristic that permits the knife to be used for good purposes - a sharp knife can just as easily be used to do harm as to do good. Sharpness is thus a functional value rather than a moral value.[139] Raz is widely and provocatively challenged on this point;[140] however, it would again be well beyond the scope this article to wade into this debate. Nor is it is necessary for our

---

government"); Id. at 225 (stating that conformity to the rule of law does not always facilitate realization of the indirect purposes of the law, but it is essential to the realization of its direct purposes).

136 Id. (reiterating that, although "the rule of law... is a necessary condition for the law to be serving any good purpose at all... conformity to the rule of law also enables the law to serve bad purposes.").

137 Id. at 224-25.

138 Id. at 226.

139 Id. at 225-26 (stating, however, that conformity to the rule of law "is virtually always of great moral value," and "[This] does not mean that conformity with [the rule of law] is of no moral importance. Quite apart from the fact that conformity to the rule of law is also a moral virtue, it is a moral requirement when necessary to enable the law to perform useful social functions; just as it may be or moral importance to produce a sharp knife when it is required for a moral purpose. In the case of the rule of law this means that it is virtually always of great moral value.").

140 See Robert P. George, Reason, Freedom, and the Rule of Law: Their Significance in Western Thought, 15 Regent U. L. Rev. 187 (2003) (discussing the disagreements between Hart, Raz, Fuller and MacCormick on the relationship between the rule of law and morality). Raz seems somewhat unresolved, as well. The relationship he describes between the rule of law and respect for human dignity is not merely one of negation; i.e., "deliberate disregard for the rule of law violates human dignity." See also Raz, supra n. 2, at 221. Conformity to the rule of law is a positive value, as well. "A legal system which does in general observe the rule of law treats people as persons.... It presupposes that they are rational autonomous creatures and attempts to affect their actions and habits by affecting their deliberations." Id. at 222. This positive value stands in contrast to Raz's statement that "[t]he rule of law is essentially a negative value." Id. at 224. This contradiction is not fully addressed.

purposes to do so. It is enough to say that conformity to the rule of law is an inherent value of the law, regardless of how characterized.

It is against this conception of the rule of law, and the analytical framework that it provides, that territorially-based governance of cyberspace will be tested. This framework includes both Raz's broad requirements and the principles derived there from, each interpreted against the basic idea that the law should be capable of guiding the behavior of its subjects. Values to the individual that are served by conformity to the rule of law will also be considered, as well as the role that the rule of law plays as an inherent functional value of law itself. In each instance, it seems that the rule of law as Raz conceives it is failing in cyberspace.

C. Testing Conformity to the Rule of Law

Johnson and Post's arguments are built on a description of a network in which data availability is simultaneous, universal and undifferentiated - a network that simply is not currently constructed such that data can be made to respect sovereign territorial borders without severe harm to the perceived value of the network.[141] That value resides, in large part, in the network's ability to provide instantaneous access to enormous amounts of digital data, to make it available to a vast online population, and to do so cheaply (albeit, largely indiscriminately). Data providers, whether by intentional distribution or simple data access, are thus exposed to the law and legal regimes of multiple sovereign jurisdictions; and by implication, overlapping, inconsistent and often contradictory regulation. Johnson and Post attempt to eliminate this conflict by defining cyberspace as a distinct sphere - a territory unto itself - and arguing that the extraterritorial application of sovereign law is invalid, focusing on a necessary relationship between sovereign and subject. At the very least, they argue, it cannot reach data providers located in foreign

[141] See Johnson & Post, supra n. 3, at 1370-71 (describing the network as follows: "Cyberspace has no territorially based boundaries, because the cost and speed of message transmission on the Net is almost entirely independent of physical location. Messages can be transmitted from one physical location to any other location without degradation, decay, or substantial delay, and without any physical cues or barriers that might otherwise keep certain geographically remote places and people separate from one another. The Net enables transactions between people who do not know, and in many cases cannot know, each other's physical location. Location remains vitally important, but only location within a virtual space consisting of the "addresses" of the machines between which messages and information are routed. The system is indifferent to the physical location of those machines, and there is no necessary connection between an Internet address and a physical jurisdiction. Although the domain name initially assigned to a given machine may be associated with an Internet Protocol address that corresponds to that machine's physical location (for example, a '.uk' domain name extension), the machine may be physically moved without affecting its domain name. Alternatively, the owner of the domain name might request that the name become associated with an entirely different machine, in a different physical location. Thus, a server with a '.uk' domain name need not be located in the United Kingdom, a server with a '.com' domain name may be anywhere, and users, generally speaking, are not even aware of the location of the server that stores the content that they read.").

countries.

It is an expansive argument, but necessarily so. Johnson and Post's true goal is some form of Internet self-governance, however that might be realized. That position requires them, it seems, to invalidate the application of existing sovereign-based power structures to online activity. Conceived as an issue of extraterritoriality, these structures are challenged less as independent regimes, but rather as horizontally coexistent systems. In truth, Johnson and Post want to free the online persona from all territorially-defined authorities. But overlapping, inconsistent and contradictory regulation does not speak to this goal. At best, it argues for limited exposure only to the laws of the territory in which the data-provider is physically located (as opposed to a conception of an on-line persona existing in a cyberspace of independent sovereignty). The validity of the relationship between territorially-based sovereign and subject remains essentially untouched.

It is this distinction that allows Goldsmith to frame his rebuttal. Multistate private law disputes are generally left to the individual countries. Although base international standards may apply, the resolution of conflicts arising from a sovereign's attempt to apply its laws extraterritorially to the subject of another is guided almost entirely by domestic rules governing jurisdiction, choice of law, and the recognition and enforcement of judgments. Insofar as the sovereign-to-subject relationship remains valid in the online context, the application of these rules serves to validate those cases in which extraterritorial regulation is upheld. In other words, if we assume that "Sovereign A" may validly regulate "Citizen A," and that Sovereign A has established regulations governing the application of foreign law to its subjects, then Sovereign A has the authority to validate the application of the law of "Sovereign B" to its citizens, including the online activities of Citizen A. Viewed this way, the problems of validity that Johnson and Post identify - exposure to multiple legal regimes, and to overlapping, inconsistent, and often contradictory regulation - are "solved" by rules (jurisdiction, choice of law, enforcement of judgments) that either validate or invalidate extraterritorial regulation.

I suggest an entirely different analysis of the issue, rooted in the rule of law. But this requires a two-part fundamental shift in perspective. First, rather than focusing on the relationship between subject and sovereign, we instead consider the relationship between law and the autonomous individual. As conceived by Raz, the basic intuition of the rule of law is that "the law should be such that people will be able to be guided by it."[142] To achieve this goal, laws must be, inter alia, adequately publicized, clear in meaning, stable and constant without frequent change, and non-contradictory.[143] Moreover, there should be no laws that are in practice impossible to follow.[144] This promotes a stable framework within which the individual may fix long-term goals and effectively direct her life towards those goals.[145] Second, and flowing from the first point, rather than evaluating

142 See Raz, supra n. 2, at 213.
143 Id. at 214-218.
144 Id. at 211-18.
145 Id. at 220.

the extraterritorial regulation of online activity as a question of validity (i.e., the validity of law and legal systems, as a corollary to the subject-sovereign relationship), we instead focus on the purposes, values and virtues of law (i.e., a normative ideal of what law ought to be). Thus, conformity to the rule of law is not a question of validity, but merely a value to be weighed in relation to other values and purposes that the law should serve.[146] Yet, its value to the individual is undeniably compelling, for "observance of the rule of law is necessary if the law is to respect human dignity"[147] by respecting individual autonomy - manifest in the individual's right and capability to control their own future - and protecting personal freedom.[148]

Admittedly, conformity to the rule of law has been traditionally analyzed against laws flowing from and enforced by territorially-based sovereigns against those within its borders. But rule of law principles need not be limited to this model. Indeed, Raz's conception refers broadly to "the government in all its actions" and the law's ability to guide "people" generally.[149] Moreover, the value of the rule of law is not based in the validating relationship between subject and sovereign, and is thus not necessarily limited by that relationship. Rather, the rule of law speaks to the relationship between law and the individual, whether within or outside the sovereign territory. It is in this relationship that the values promoted by the rule of law are to be realized.

Applying these principles to the governance of cyberspace, we begin with the normative ideal: That legal regimes asserting their authority to apply their laws across borders should conform that assertion to the rule of law. This leads, initially, to two questions. First, assuming that the online data provider is likely, within the current architecture of the Internet, to be simultaneously exposed to innumerable legal regimes, does that exposure establish a presumption that these multiple assertions of authority fail to conform to the rule of law? Second, and building on this first point, is conformity to the rule of law nevertheless preserved - despite the inconsistency and contradiction apparent on the face of it - by rules governing jurisdiction, choice of law, and the recognition and enforcement of judgments?

Initially, the answer to the first question seems rather simple. As a practical matter, the larger legal regime governing online activity consists of an uncoordinated collection of otherwise independent territorially-based legal regimes. If data reaches (or is capable of reaching) a data recipient physically located in a particular territory, and that data thus produces (or threatens to produce) a regulated "effect" within that territory, the data provider is potentially subject to liability arising from that effect. This is true for each territory within the network. Almost by definition, then, the uncoordinated and

---

146 Id. at 222 (observing "[c]onformity to the rule of law is a matter of degree" and "the undoubted value of conformity to the rule of law should not lead one to exaggerate its importance."); See also infra, n. 193-95 and referenced text.

147 Id. at 221.

148 Id.

149 Id. at 210, 213 (quoting F.A. Hayek, The Road to Serfdom, 54 (Routledge Press 1944)).

duplicitous "law" of cyberspace is inherently contradictory and in practice impossible to follow. Likewise, the law of these individual legal regimes is often inadequately publicized outside of territorial boundaries, leaving the data provider with no knowledge of what the law governing a particular behavior "is." Moreover, the application of multiple legal regimes to online data flowing simultaneously through and across borders without differentiation challenges the ideal that law be reasonably stable, constant, and adequately noticed when changed. The various independent territorially-based legal regimes might themselves be stable, but the overarching law governing one's online behavior changes almost instantaneously as the data moves through the network, entirely without notice.

Thus, where the Internet is understood as an undifferentiated and pervasive environment in which actions are simultaneously subject to innumerable territorially-based legal regimes, it is the perceived threat of arbitrary power - that which inherently arises from primary rules of obligation that are uncoordinated, duplicitous, contradictory, inadequately publicized, as a practical matter unstable and inconsistent, and in practice impossible to follow - that poses the greatest threat to individual autonomy and human dignity. For instance, imagine that you were able to gather a comprehensive list of all of the laws of all the countries in which the Internet is available, and that you were somehow able to cross-reference these laws such that you were able to identify all laws that would apply to a particular act. Assuming the principle that people should be ruled by the law and obey it,[150] if any of those laws prohibit the particular activity (regardless of the legal regime from which the law originates), then you should not engage in the activity - even if the vast majority of legal regimes permit the act. But what if one legal regime requires a certain act, while another prohibits it? Your only choice is to avoid the Internet altogether, eliminating your exposure to multiple legal regimes.

In reality, of course, one cannot practically know all of the laws of all the countries in which the Internet is available. Indeed, it would not be feasible to know even the laws applicable to one particular act. Thus, with each online activity we expose ourselves to the threat of arbitrary power. It is not simply that our choices are diminished, although they are, but rather we cannot know the legal consequences of our actions. Conformity with the rule of law serves the ideal that law should be capable of guiding the behavior of its subjects.[151] But the value of this guidance to the individual is not that the rule of law limits the greatest range of behavior - in fact, the threat of arbitrary power might most effectively accomplish such a goal. Rather, the value of the rule of law is to provide a certain degree of stability and certainty, such that in the making of both short-term decisions and long-term plans the individual has the effective ability to choose between as many options as possible[152] (inasmuch as the law can provide). In this way, conformity with the rule of law seeks to protect personal freedom and individual autonomy, and to

[150] Id. at 213.
[151] Id. at 214.
[152] Id. at 220.

promote human dignity.[153] The overarching legal regime imposed in the online environment - essentially comprised of an uncoordinated multitude of independent regimes with competing claims of authority - thus fails to conform either to the principles of the rule of law or to the values it promotes.

The question might then become whether this apparent failure to conform to the rule of law in the online environment is somehow "cured" by rules governing jurisdiction, choice of law, and the recognition and enforcement of judgments. This was, in essence, Goldsmith's response to Johnson and Post's overly-ambitious attack on the validity of extraterritorial regulation. But to apply this conception here would be to ignore several important distinctions. First, as an analytical matter, the Johnson-Post-Goldsmith debate focused on the validating relationship between subject and sovereign, while the normative ideal of the rule of law focuses on the relationship between law and the autonomous individual. Moreover, the normative question is not one of validity, but of the purposes, values and virtues of law.

With these basic distinctions in hand, what emerges is a key difference of perspective. Put simply, the point of reference against which the question of validity is judged, is entirely separate from that invoked by conformity to the rule of law. The question of regulatory validity, as Johnson and Post present it, is linked to the issue of enforcement. Indeed, they refer to the power of enforcement as "a defining attribute of sovereignty and statehood."[154] Thus, if the extraterritorial regulation of cyberspace is to be invalid, then that "violation" must occur at the time of illegitimate enforcement against the extraterritorial actor, after completion or attempted completion of the objectionable act. It is not enough to say simply that the mere threat of enforcement renders extraterritorial regulation invalid. Thus, as Goldsmith argues, the rules of jurisdiction, choice-of-law, and the recognition and enforcement of judgments - developed within the authority of the sovereign-subject relationship and applied to the very question of coercive enforcement - are sufficient to validate (as Johnson and Post describe it) acts of extraterritorial regulation.

Conformity to the rule of law is judged, both in principle and in its value to the individual, against an entirely different reference point. The question is not whether post-act/attempt regulatory enforcement is valid, but rather whether the undifferentiated and unknowable threat of arbitrary power undermines the normative ideal and its value to the individual. As Raz describes it, conformity to the rule of law enables the individual "to foresee with fair certainty how the authority will use its coercive powers in given circumstances."[155] In this stable framework of relative certainty, the individual may fix long-term goals and effectively direct her life towards those goals.[156] Thus, the value is in

---

153 Id. at 220-22.

154 See Johnson & Post, supra n. 3, at 1369.

155 See Raz, supra n. 2, at 210, 213 (quoting F.A. Hayek, The Road to Serfdom 54 (Routledge Press 1944)).

156 Id. at 220.

the act of choice itself, free from the perceived threat of arbitrary power - promoting the dignity of individual autonomy - rather than at the point of adjudication and enforcement. If the threat of undifferentiated and arbitrary power inherent in the prevailing system of competing claims of authority thus deprives the individual of the effective ability to choose between as many options as possible, then the value of conformity to the rule of law is already lost and cannot be restored at the point of enforcement.

This nevertheless raises the issue of whether domestic rules of jurisdiction, choice-of-law, and enforcement, when stable and consistent, can effectively dispel the perceived threat of arbitrary power, thus preserving conformity to the rule of law despite the arguable risks. To this end, it may be helpful to imagine a greatly simplified process timeline, starting with an individual's consideration of what potential actions are available. She weighs the perceived risk, cost and benefit of each, then makes a choice and acts. At some later point, she may be subject to regulation and enforcement stemming from that act. For the individual, the value of conformity to the rule of law is actualized most clearly at the moment of choice, and then through the period of potential enforcement as the act brings relatively predictable results. Thus, the value is realized both through the individual's perception at the moment of choice as to what alternatives are effectively available, and then as the authority acts in accordance with her understanding of how it will use its coercive powers in a given circumstance. The individual's perception is not, of course, based upon certainties but is instead a consideration of risk. In the context of multiple assertions of authority over online activity, that risk may be somewhat diminished by domestic rules of adjudication and enforcement applicable to the ultimate imposition of authority,[157] but the perception of heightened risk and uncertainty in the process of choice remains.

The question, then, is whether the perception and potential for risk inherent in such an environment - comprised of a multitude of independent, uncoordinated regimes with competing claims of authority, but subject to domestic rules of enforcement - can itself create a threat of arbitrary power such that it fails to conform to the rule of law. In this consideration, it is again vitally important to recall that this challenge to extraterritorial regulation is not so demanding as one of validity. The normative ideal of the rule of law is just that - an ideal or value to be weighed along with the other values and purposes of law. The point is not that one may be ultimately vindicated, but that the individual will be unable to act in the first place because the threat is such as to effectively deny the choice. And this, I believe, is where the question turns. The value of conformity to the rule of law is one of degree.[158] And as individuals gain a global "presence," and that presence itself gains value (mirroring the perceived value of the network), secondary rules of post-act enforcement are simply inadequate to answer a threat of perception. The online actor cannot know, as a practical matter, the many laws applicable to a particular act, nor when one or more sovereign may decide to attempt regulatory action. This is particularly true in those areas of regulation in which morality, religion and culture are at their most

[157] See Goldsmith I, supra n. 3, at 1208, 1212-37, 1239-42.
[158] See Raz, supra n. 2, at 228.

influential, such as speech, race, sex, and even intellectual property. Moreover, it is not simply one actor or a few legal systems. It is an exponential multitude. If the value of the network lies in its ability to provide instantaneous access to enormous amounts of digital data, to afford every individual with the opportunity to provide that data, to make it available to a vast online population, and to do so cheaply, then these values must inform our understanding of what conformity to rule of law requires in cyberspace.

III. AND IF THE RULE OF LAW FAILS IN CYBERSPACE, WHAT THEN?

As I suggested at the outset, this article is not intended as an all-embracing account of extraterritorial regulation in cyberspace. My aim is simply to recommend a different perspective on the normative debate of borders and territorial sovereignty. Nevertheless, a few thoughts on potential consequence and response may be helpful.

First, it bears re-emphasis that the Johnson-Post argument, pressed ultimately as an issue of validity, was in essence a zero-sum game. As Johnson and Post constructed their challenge, the extraterritorial regulation of online activity by territorially-based sovereigns is either valid or invalid. There is no middle ground or balancing of interests. The rule of law is, by comparison, "just one of the virtues that law should possess . . . to be balanced against competing claims of other values."[159] Although "[i]t is generally agreed that general conformity to the rule of law is to be highly cherished . . . one should not take the value of the rule of law on trust nor assert it blindly.[160] As Raz recognizes:

> Conflict between the rule of law and other values is just what is to be expected. Conformity to the rule of law is a matter of degree, and though, other things being equal, the greater conformity the better - other things are rarely equal. A lesser degree of conformity is often to be preferred precisely because it helps the realization of other goals.[161]

Thus, far from excluding our ideas regarding the value of the network, the issue of conformity to the rule of law invites concomitant consideration of relevant social goals - whether as a libertarian view of cyberspace or cultural condemnation of particular types of speech - as inherent to the normative ideal.

Indeed, it can be argued that conformity to the rule of law is inextricably linked to the very virtues of the Internet that we celebrate. If the value of the network indeed resides (in the most general sense) in its scope, ease of data access and provision, minimal barriers to entry, and liberty of action, then conformity to the rule of law is central to the realization of social goals reflected in that value. If we cannot know what response our actions will bring - if the law of cyberspace consists of multiple sovereign systems with competing claims of authority, if on the whole the law of that overarching

---

159 Id. at 228.
160 Id. at 222.
161 Id. at 228.

regime is inconsistent and often contradictory, if this exposes the perceived threat of arbitrary power - then we risk incapacity within the online environment. This arguably serves neither the value of the network (a necessarily contingent argument), nor the ideal of individual autonomy that facilitates the effective ability to choose between as many options as possible.

Admittedly, there is an acute danger of falling into the very trap that Johnson and Post failed to avoid - relying upon a distinct description of the Internet (whether libertarian or otherwise) as a necessary component of the argument. But here the question of conformity to the rule of law is not dependent upon a particular conception of the network. To the contrary, it is the value of the rule of law that should inform our choices of what the network should be. If we are to truly regard and promote conformity to the rule of law then we must identify those values and/or goals of society against which such conformity is to be weighed. As such, the normative ideal requires us to confront our vision of and for the Internet. Only then may we truly determine to what degree conformity to the rule of law is to be pursued at the expense of other values, and how such conformity might be advanced. Should we seek some sort of international regime in which regulation of certain online activity is harmonized? Or should legal regimes that fail to conform their regulation of online activity be rejected by the user's home country, placing the burden on the state to regulate upstream from the domestic data recipient? The answers to these questions are predicated on choices that have yet to be made, but which are compelled by a commitment to the rule of law.