OF NODES AND POWER LAWS: A NETWORK THEORY APPROACH TO INTERNET JURISDICTION THROUGH DATA PRIVACY

Andrea M. Matwyshyn∗

INTRODUCTION

The question of whether the Internet presents unique legal concerns has been much debated,[1] as has, specifically, whether Internet-related harms warrant a fundamentally different personal jurisdiction paradigm.[2] As a consequence, courts within the United States have not adopted a uniform approach to personal jurisdiction in cases arising out of Internet activity.[3]

∗ Clinical Assistant Professor of Law, Northwestern University; Affiliate, Centre for Economics and Policy, University of Cambridge. The author invites comments at a-matwyshyn@law.northwestern.edu and wishes to thank Martin H. Redish, Sharon M. Gordon, and Cem Paya for their insightful commentary and critiques.

1 *E.g.*, *compare* Frank Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, *with* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999).

2 *See, e.g.*, Patrick J. Borchers, *The Problem with General Jurisdiction*, 2001 U. CHI. LEGAL F. 119, 137 (arguing that the concept of general jurisdiction is fatally flawed, particularly in the context of the Internet, but should not be abandoned); Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345 (2001) (arguing for a targeting approach rooted in *Calder*); Henry H. Perritt, Jr., *Towards a Hybrid Regulatory Scheme for the Internet*, 2001 U. CHI. LEGAL F. 215, 215 (arguing for private ordering as the primary governing construct of Internet activity within broad public law frameworks as a hybrid system of regulation); Martin H. Redish, *Of New Wine and Old Bottles: Personal Jurisdiction, the Internet and the Nature of Constitutional Evolution*, 38 JURIMETRICS J. 575, 609 (1998) (arguing for a balancing test that would weigh a meaningful constitutional due process standard for procedural fairness to the defendant against a state's interest as the dispositive inquiry in Internet jurisdiction cases); Allan R. Stein, *Frontiers of Jurisdiction: From Isolation to Connectedness*, 2001 U. CHI. LEGAL F. 373 [hereinafter Stein, *Frontiers of Jurisdiction*] (arguing for harnessing technology to determine geographic location to permit defendants to refrain from entering a forum and setting forth theoretical bases for jurisdictional authority); Allan R. Stein, *The Unexceptional Problem of Jurisdiction in Cyberspace*, 32 INT'L LAW. 1167 (1998) [hereinafter Stein, *Jurisdiction in Cyberspace*] (arguing that Internet jurisdiction issues can be understood within a territorial framework); Mary Twitchell, *Why We Keep Doing Business with Doing-Business Jurisdiction*, 2001 U. CHI. LEGAL F. 171 (arguing that we should retain doing-business jurisdiction even in light of the Hague Convention and problems posed by the Internet).

3 *Compare* Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996), *with* Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997), *and* GTE New Media Servs., Inc. v. BellSouth Corp., 199 F.3d 1343 (D.C. Cir. 2000).

Further, international consensus on the matter is lacking.[4] What remains clear, however, is that questions of jurisdiction arise at the epicenter of the intersection of technology-mediated commerce and social governance; jurisdictional determinations tacitly address the social balance between providing incentives for entrepreneurship and providing recourse for harms. Through jurisdictional determinations, our courts make assessments regarding the social value of competing economic and personal interests. Striking and maintaining a jurisdictional balance between entrepreneurship and recourse becomes increasingly complex in the context of new types of harms that arise as a consequence of new methods of conveying information and conducting commerce.[5]

In this Article, I introduce a "Trusted Systems" approach to jurisdiction determinations in cases involving allegations of intentional torts and intellectual property infringement that occur through information technology mediated communication networks ("Network Communications").[6] This approach hopes to address the flaws of previous Internet-specific jurisdictional frameworks: technological over-determinism and lack of intellectual grounding in traditional jurisdictional precedent. The Trusted Systems approach is a departure from existing approaches because it relies on the naturally occurring structure of human-network communication as the basis for crafting a jurisdictional paradigm. Similarly, it is novel in its intellectual reliance for jurisdictional deep structure on notions of responsibility and consent. It is not novel in its firm grounding and respect for traditional jurisdiction doctrine and minimum contacts analysis. Therefore, unlike the "Internet"[7] jurisdiction paradigms currently in widespread use by courts, the Trusted Systems approach provides firmer grounding for the future evolution of jurisdiction precedent in cases involving alleged harms arising out of new media. I conclude by extrapolating the argument to other technology regulation contexts, urging recognition of the importance of all technology regulation acting in tandem with the naturally occurring structures of human-network communications.

It might be said that all jurisdictional determinations in civil cases ultimately involve questions of dynamic information transfer, specifically whether the defendant knew or should have known that he or she might be haled into the courts of a particular forum and whether the plaintiff had rea-

4 *See, e.g.*, Linda Silberman, *Comparative Jurisdiction in the International Context: Will the Proposed Hague Judgments Convention Be Stalled?*, 52 DEPAUL L. REV. 319, 335–37 (2002).

5 For a discussion of striking a balance between social incentivization of entrepreneurship and providing recourse for harm, see, for example, Howard H. Chang et al., *Some Economic Principles for Guiding Antitrust Policy*, 1998 COLUM. BUS. L. REV. 223.

6 These two categories of cases constitute the vast majority of cases presenting murky jurisdiction waters in inquiries involving information technology-mediated network communications. *See infra* Part II.

7 The current frameworks referred to as Internet jurisdiction frameworks actually relate only to the World Wide Web, not the Internet as a whole. *See infra* discussion accompanying note 92.

son to believe that recourse was available in that forum. Therefore, the goal of a successful jurisdictional regime, particularly in the context of harms arising out of Network Communications, is to maintain the stability of the "trusted system"[8] of fair, truthful information exchange in society, regardless of whether the information in question addresses an impending commercial transaction between two parties (and the likelihood that a boiler will explode) or a celebrity's private life. To accomplish this end, courts seek or should seek to maximize predictability in jurisdictional outcomes. Jurisdictional determinations can provide clear behavioral cues to actors regarding the extent of their social responsibilities in connection with fair information practices to particular forums. Simultaneously, these cues provide actors with certainty about the ability to be called or to call someone else in front of a particular court system. In other words, a successful jurisdictional regime is one that both preserves the trusted system of information exchange and enables actors to control their exposure to liability in particular jurisdictions, while planning on the ability to seek redress for harms caused to them. Current Internet jurisdiction frameworks accomplish neither, particularly in the context of intentional torts and intellectual property-related harms that occur as a consequence of Network Communications.

As Internet penetration within the United States currently exceeds 50 percent of the population,[9] it is essential that we acknowledge that Network Communications present fundamental challenges to existing jurisdictional frameworks. The correct solution to these challenges is not to apply the "band-aid" approach of new technology-specific[10] standards that has been used to date, nor is it necessarily desirable to stretch existing, but potentially suboptimal constitutional precedent to tenuous extremes. I submit that the correct approach to addressing the fundamental challenges presented by Network Communications to jurisdiction paradigms is to contemplate the medium as a whole and return to the jurisdictional starting point of a traditional minimum contacts analysis, tempered with a procedural due process overlay. We must assess current and foreseeable communication networks as dynamic environments of information transmission within and with which groups of actors interact; we need to ask how their organiza-

8 In computing terminology, trusted computing bases are the components in a system that make the system secure and generally include, among other things, provisions for regulating access of users, granting authorization for using specific resources, and protecting against system infiltration. Trusted systems are regularly tested or verified. *See* Tech Target Network, Glossary: Trusted Computing Base, *at* http://searchvb.techtarget.com/gDefinition/0,294236,sid8_gci816161,00.html (last updated Apr. 28, 2003).

9 NAT'L TELECOMMS. & INFO. ADMIN. & ECON. & STATISTICS ADMIN., U.S. DEP'T OF COMMERCE, A NATION ONLINE: HOW AMERICANS ARE EXPANDING THEIR USE OF THE INTERNET, ch. 2 (2002) [hereinafter NTIA], *available at* http://www.ntia.doc.gov/ntiahome/dn/html/Chapter2.htm.

10 The Internet presents only one type of network technology that can mediate communications. Crafting a technology-specific standard increases the likelihood that the standard will be made irrelevant by subsequent technological innovation.

tional structures differ from and influence those of the physical space in which our previous jurisdictional frameworks are rooted. Following such an inquiry, we can then embark towards a merger of these two worlds in our jurisdiction paradigms.

Since 1997, the leading jurisdiction standard within the United States, a technologically over-determined World Wide Web-specific standard, has been a "sliding scale" approach[11] that was first articulated in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc*.[12] However, it has become increasingly clear that this sliding scale approach has limitations to its usefulness as a framework.[13] As a consequence, the sliding scale approach is, at least by some reports,[14] falling out of favor with both courts and legal practitioners. [15] Its inconsistent application by different courts[16] offers little guidance to other courts. Similarly, for technology transactions counsel who are attempting to advise clients on limiting liability, the sliding scale approach provides little comfort or predictability because the approach's reliance on the premise of large variations in websites' degree of "interactivity" is being rendered meaningless. Network Communications increasingly involve user-invasive, Internet data collection capabilities that are invisible to most users.[17] Courts are progressively replacing or supplementing the sliding scale approach with the focal point, or center of gravity, approach[18] adopted as the "effects test" of *Calder v. Jones*[19] or a derivative "targeting" test.[20]

11 See *infra* note 92.
12 952 F. Supp. 1119 (W.D. Pa. 1997).
13 For example, under a sliding scale jurisdictional analysis, a defamatory but "uninteractive" website would never provide an adequate basis for jurisdiction in a defamed plaintiff's forum, even if the plaintiff has suffered severe reputational injury. For a discussion of various limitation of the sliding scale approach, see Michael Traynor & Laura Pirri, *Personal Jurisdiction and the Internet: Emerging Trends and Future Directions*, 712 PRACTICING L. INST. 93, 113–20 (2003) and Geist, *supra* note 2.
14 Not all commentators agree that the sliding scale approach is losing a following. As a practical matter, courts usually start with a sliding scale approach analysis. *See, e.g.*, Denis T. Rice & Julia Gladstone, *An Assessment of the Effects Test in Determining Personal Jurisdiction in Cyberspace*, 58 BUS. LAW. 601, 652 (2003).
15 *See, e.g.*, Traynor & Pirri, *supra* note 13, at 113.
16 For further discussion, see Rice & Gladstone, *supra* note 14, at 622–27.
17 One such technology is a "web bug." A web bug, also known as a "pixel tag," "web beacon," or "clear GIF," is a 1x1 pixel image embedded in html code. If a web bug is present, instead of simply fetching an image, a server invokes a CGI program that logs information about the user's actions. *In re* Pharmatrak, Inc. 329 F.3d 9, 14 (1st Cir. 2003); *see also In re* Doubleclick Cases, No. JC4120, 2001 WL 1029646 (Cal. Super. Ct. June 11, 2001); *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).
18 *See* Albert A. Ehrenzweig, *The Transient Rule of Personal Jurisdiction: The "Power" Myth and Forum Conveniens*, 65 YALE L.J. 289 (1956).
19 In *Calder v. Jones*, 465 U.S. 783, 783–84 (1985), an entertainer sued a tabloid and the authors of an allegedly defamatory article. The Court found that, because the tabloid's circulation was large in California and because the authors of the article had knowledge that the entertainer resided in California, a state regarded as a center for the entertainment industry, the authors were deemed to have knowledge that their article would have an effect in the state of California. Thus, jurisdiction was found to be proper in California over both the tabloid and the authors of the allegedly defamatory article.

However, these approaches, which are intellectually grounded in *Calder*, are similarly inferior and, particularly when applied to Internet publications, provide no certainty for limiting liability.[21] Meanwhile, they may unnecessarily chill speech.

This Article conducts a two-fold inquiry. First, Part I argues that the mainstreaming of Network Communications in the last decade through the Internet, a type of information technology-mediated communication network, presents a challenge to existing jurisdiction paradigms in the context of cases involving allegations of intentional torts and intellectual property harms because it has exerted a fundamental structural shift on the conception of collective economic identity[22] in the United States. This shift in economic identity results from two phenomena: (1) the heightening of the economic value afforded data and, consequently, data privacy; and (2) the reconstruction of the concept of "corporate identity" in a more egalitarian manner. This two-part reconceptualization of economic identity is, correspondingly, driving a change in the way that harms to persons and their property occur in an inherently transnational global medium. Therefore, I would submit that our current Internet jurisdiction paradigms, which were developed primarily in the context of intentional torts and intellectual property-related harms, are inadequate in connection with allegations of such harms. This inadequacy exists in part because our Internet jurisdiction paradigms have not recognized the shift in construction of economic identity.

Second, Part II concurs with the point, as discussed by numerous authors, [23] that it should not be a foregone conclusion that an Internet-specific standard, that disregards the majority of prior jurisdiction precedent, is essential. Traditional jurisdictional standards provide useful, even if not adequate, guidance for jurisdictional dispositions in cases alleging harms involving Internet activity. Building on this scholarship, this Article calls for the abandonment of both the sliding scale approach and the effects test/targeting approach in the context of claims alleging intentional torts or intellectual property-related harms involving Network Communications, such as communications through the Internet. I suggest that the United States start over in its jurisdictional approach by using a traditional minimum contacts analysis through a new approach grounded theoretically in

20 *See, e.g.*, Young v. New Haven Advocate, 315 F.3d 256, 262–63 (4th Cir. 2002), *cert. denied*, 123 S. Ct. 2092 (2003).

21 Traynor & Pirri, *supra* note 13, at 147.

22 For a discussion of individual identity and its (re)construction in light of technology, see PAULINA BORSOOK, CYBERSELFISH (2000); THE CYBORG HANDBOOK 364 (Chris Hables Gray ed., 1995); FROM BARBIE TO MORTAL KOMBAT 294 (Justine Cassell & Henry Jenkins eds., 1998); THE GENDERED CYBORG 217 (Gill Kirkup et al. eds., Open Univ. 2000); N. KATHERINE HAYLES, HOW WE BECAME POSTHUMAN (1999); SHERRY TURKLE, LIFE ON THE SCREEN (1995).

23 *See, e.g.*, Stein, *Jurisdiction in Cyberspace*, *supra* note 2 (arguing that Internet jurisdiction issues can be understood within a territorial framework).

consensual social responsibility, rather than either a strictly contractarian[24] or regulatory[25] model of jurisdiction. Such a middle ground approach is proposed here, turning on and recognizing network user data as a commodity with market value[26] and operationalizing the moment of jurisdiction over a defendant as a bright line standard depending on data collection. This social responsibility approach falls in between the two dominant models of jurisdiction, incorporates positives of both, and more accurately reflects the shift in construction of economic identity and the level of agency of both content providers and users of Network Communications.

Thus, this Article proposes a framework for harmonizing jurisdictional treatment of different kinds of cases involving allegations of intentional tort and intellectual property harms in connection with Network Communications. This framework, which is rooted in a minimum contacts analysis, shifts away from both the sliding scale approach and an effects/targeting test towards a more traditional minimum contacts analysis. I advocate adoption of what might be termed a "Trusted Systems"[27] approach to jurisdiction; it is premised on notions of proportional social responsibility and consent of both individual economic actors and states on the theoretical level, operationalized through a bright-line standard based on user data on the practical level. The proposed Trusted Systems approach incorporates lessons of network theory[28] regarding the relative importance of different types of actors within structures of network-user interactions, as well as the unique roles of "nodes" and "hubs" within the network and their proportional effects on the survival and stability of systems. In adopting such an approach, the Internet jurisdiction framework for intentional torts and intellectual property harms will move toward a standard more in line with a traditional minimum contact analysis, based on receipt by the defendant of economic value from a forum.

Finally, I assert that the problems of Internet jurisdiction in intentional tort and intellectual property cases demonstrate a broader problem in how

24 *Id.* at 375.
25 *Id.*
26 For a discussion of the transformation of user data into a marketable commodity, see, e.g., Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000).
27 It can be argued that courts function in a manner similar to trusted computing bases through jurisdiction. Using jurisdictional determinations, courts control access of certain plaintiffs to adjudication of claims in certain courts. Jurisdiction dispositions prevent the clogging of court dockets by claims that do not bear an immediate relevance to the interests of the forum state, thereby preventing a systemic infiltration of sorts. Finally, just as trusted computing systems must be regularly tested and verified, so should the correctness of jurisdiction approaches espoused by courts. For a discussion of trusted computing, see, for example, Ross Anderson, 'Trusted Computing' Frequently Asked Questions, *at* http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html (last visited Aug. 2003).
28 ALBERTO LASZLO BARABASI, LINKED (2002). Network theory is different from the economics concept of network effects. For a discussion of network effects, see Max Schanzenbach, *Network Effects and Antitrust Law: Predation, Affirmative Defenses, and the Case of* U.S. v. Microsoft, 2002 STAN. TECH. L. REV. 4.

we theorize and regulate Network Communications. A conceptual shift is needed in order to bring the structural reality of networks and organizational behavior within the network to bear on the jurisdictional and other laws seeking to govern them. Studying the structure of computer code, the structure of information technology law, or individual government behaviors without contemplation of the legal strategy and organizational behavior phenomena occurring in connection with Network Communications eliminates a critical component of the analytical calculus. The patterns of these group constructs[29] and dynamic strategic behaviors and interactions might be termed the "Organizational Code" of networks, as opposed to the computer code,[30] regulatory code,[31] or value code[32] that also governs them. It is only by being sensitive to and studying this Organizational Code, which represents the iterated, relational interactions of different groups of actors—both human and otherwise—as they actually occur within and about Network Communications, that effectual legal code can arise to preserve social order while minimizing damage to the network.

I. THE EFFECT OF NETWORK COMMUNICATIONS ON CONSTRUCTION OF ECONOMIC IDENTITY

The macroeconomic issue of whether a new national "Internet" economy exists (or ever existed) in the United States has been one of hot debate for many years now.[33] Three significant trends are undeniable, however: (1) the growing numbers of people in the United States with Internet access;[34] (2) the growing consumer spending through e-commerce;[35] and (3) the growing number of people in the United States who are not just Internet users, but Internet content producers and entrepreneurs.[36] From these three trends alone, it is evident that a change has occurred in the way that people

29 One such organizational group construct is group identity.
30 LAWRENCE LESSIG, CODE 53 (1999).
31 *Id*.
32 Yochai Benkler, *Internet Regulation: A Case Study in the Problem of Unilateralism*, 11 EUR. J. INT'L L. 171, 172, 177 (2000).
33 *E.g.*, *compare* Kevin Kelly, *New Rules for the New Economy*, WIRED, Sept. 1997, http://www.wired.com/wired/archive/5.09/newrules.html ("This emerging new economy represents a tectonic upheaval in our commonwealth, a social shift that reorders our lives more than mere hardware or software ever can. It has its own distinct opportunities and its own new rules. Those who play by the new rules will prosper; those who ignore them will not."), *with* JOHN CASSIDY, DOT CON (2002) (discussing, in the words of the book's cover, "[h]ow America [l]ost its [m]ind and [m]oney in the Internet [e]ra" through irrational technological overexuberance).
34 *See* NTIA, *supra* note 9, ch. 2.
35 *See* Christopher Saunders, *Consumer Confidence in Internet Grows*, e-commerce-guide.com, *at* http://ecommerce.internet.com/news/news/article/0,,10375_1472681,00.html (last updated Sept. 30, 2002).
36 The number of websites is expected to double within the next five years. Raju Chellam, *Big Jump Seen in IT Spending Next Year*, IT AsiaOne, *at* http://it.asia1.com.sg/newsdaily/news009_20011015.html (Oct. 15. 2001).

in the United States spend money and otherwise participate in the economy. This shift in economic identity is inextricably interwoven with two phenomena: (1) the heightening of economic value afforded data and, consequently, data privacy; and (2) the reconstruction of the concept of "corporate identity" in a more egalitarian manner.

A. The Rise of Privacy and the Heightened Commercial Value of User Data

During the last decade, the rise of widespread Internet access has caused consumers to reevaluate the importance of control over personal information within our society.[37] In 1996, three years after the Mosaic browser was launched[38] and four years after many college students received access to their first email accounts,[39] questions of data control and privacy began to gain momentum as issues of heightened legal and national importance within the United States,[40] both among consumers and corporate entities.

As consumers increasingly ventured online to engage in information sensitive activities, such as checking bank balances or transmitting credit card information in connection with purchases, issues of data privacy and security entered their thoughts as a consequence of a medium that was novel to them.[41] Meanwhile, corporate entities had begun to place a premium on consumer information databases and to change the way consumer data is valued in corporate acquisitions.[42]

Internet privacy also began to come to the forefront of business and legal consciousness in the United States in 1996, partially as a result of international influences. In 1995, the European Union passed the E.U. "Data Directive,"[43] which contains provisions that prohibit transfer of the data of

[37] *See* H.R. REP. NO. 106-74, pt. 3, at 106–07 (1999).
As a result of the explosion of information available via electronic services such as the Internet, as well as the expansion of financial institutions through affiliations and other means as they seek to provide more and better products to consumers, the privacy of data about personal financial information has become an increasingly significant concern of consumers.
Id.

[38] Mosaic was developed by Marc Andersen and Eric Bina, two University of Illinois graduate students, in 1993. Immediately following the launch of Mosaic, use of the World Wide Web increased. *See* CASSIDY, *supra* note 33, at 51.

[39] Northwestern University first-year students entering in 1992 were the first to receive email accounts.

[40] For example, running a search by "consumer /10 data /10 privacy" in Westlaw's JLR database on December 10, 2003 brought back 343 hits. Of these hits, thirteen occurred prior to 1996, with the remainder occurring in 1996 and later.

[41] *See, e.g.*, SUSANNAH FOX, PEW INTERNET & AMERICAN LIFE PROJECT, TRUST AND PRIVACY ONLINE: WHY AMERICANS WANT TO REWRITE THE RULES 2 (2000), *available at* http://www.pewinternet.org/reports/toc.asp?Report=19.

[42] *See, e.g.*, Jane Kaufman Winn & James R. Wrathall, *Who Owns the Customer? The Emerging Law of Commercial Transactions in Electronic Customer Data*, 56 BUS. LAW. 213, 233 (2000).

[43] Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 38 [herein98:

any European person outside the European Union without consent and that require a minimum level of care in handling be contractually imposed on third parties receiving the data.[44] Although the Data Directive did not take effect until November 1998 at the earliest,[45] multinational business interests in the United States were concerned, as they were beginning to increase investment in network information technology and many had already established websites.[46]

In the legal private sector in the late 1990s, the technology bubble turned the life of every technology transactions attorney into a frenzy of

after Council Directive]. This Data Directive sets forth specific minimum standards of care in processing, handling, and storing "personal data" relating to an identified natural person and mandates that consent must be "unambiguously given" by the subject of data collection. The subject must be informed of the identity of the "controller" of the collected information, the purposes and use of collection, along with such additional disclosures as required to provide full and fair disclosure of information practices of the collector. The subject must retain the ability to access the collected personal data in order to correct or remove information. Member states of the European Union are required to enact legislation in order to codify the minimum standards of data protection articulated in the Data Directive and to provide recourse to individual subjects through judicial remedies and rights to compensation for violations of the Data Directive and corollary member-level statutes. The Data Directive provides a "floor" of protection and does not restrict E.U. members from providing higher levels of data protection to their citizens. For example, the United Kingdom Data Protection Act of 1998, which supercedes the previously enacted Act of 1984, was passed as the United Kingdom enactment of the Data Directive. *See, e.g.*, Baker & MacKenzie, European Union Directive: Country by Country Comparison Table, http://www.bmck.com/ecommerce/directivecomp6.htm (last updated Aug. 12, 2002). The 1998 Act embodies principles that cover both facts and opinions about individuals and calls into question the intentions of the data controller toward the individual with some permitted exceptions. Imposed obligations include obligations to (1) process data fairly and lawfully; (2) collect data only for specified, disclosed and lawful purposes; (3) collect data in an adequate, relevant, and not excessive manner in relation to the purposes of the collection;
(4) keep accurate and updated information where necessary; (5) retain data no longer than necessary for the purposes for which it is processed; (6) process in accordance with data subjects' rights; (7) keep collected data secure with appropriate safeguards including both technological and physical security measures; (8) prevent transfer to a country outside the European Union unless the country ensures an adequate level of protection for subject data. The Data Protection Act of 1998 further provides individual data subjects with rights that include rights (1) to be informed by a data controller whether the data controller processes and shares any of the data; (2) to require the data controller to stop or not begin processing for, among other reasons, direct marketing purposes or if processing is likely to cause harm; (3) to require the controller to correct or erase inaccurate data; and (4) to obtain compensation for damages related to data collection and processing. Pursuant to amendments to the 1998 Act, U.S. companies conducting business in the United Kingdom ("UK") are subject to the Act. Transfers of UK employee, customer, and subscriber information to the U.S. is regulated as if such data were processed in the UK, both in digital and manual form. *See* Data Protection Act, 1998, c. 29, §§ 17-21 (Eng.), *available at* http://www.hmso.gov.uk/acts/acts1998/80029--c.htm#17. The European Union has provided standard contractual clauses to assist entities in adequately protecting subject information under the Data Directive and are available from the International Chamber of Commerce at http://www.iccwbo.org/home/statements_rules/statements/2001/contractual_clauses_for_transfer.asp.

44 Council Directive, *supra* note 43, art. 17.

45 *Id.* art. 32, § 1 (mandating compliance by the Member States within three years from a state's date of adoption).

46 The Internet Archive's Wayback Machine catalogues old versions of Web sites. For example, Microsoft's MSN site dates back to at least October 22, 1996 and can be viewed at http://web.archive.org/web/*/http://www.msn.com.

questions without clear answers, particularly in connection with potential privacy liability and privacy policies.[47] Websites were engaging in significant data collection activities from traffic by U.S. and other World Wide Web ("Web") users, but the possible price tag of liability was not known. Rather interestingly, it tended to be clients, and not attorneys, who insisted that privacy policies be included on websites. No U.S. online privacy regulation mandated disclosure of data collection practices in the late 1990s.

However, despite the lack of any legal disclosure obligation and the potential for additional liability, clients in most instances proceeded to post privacy policies for reasons of public relations, frequently ignoring advice of counsel. It was subsequent to this privacy policy movement arising out of the private sector that Congress passed legislation requiring online privacy policy disclosures in connection with children's data[48] and financial data.[49] This voluntary disclosure was part of a broader industry effort to address public relations concerns about privacy and an attempt to forestall regulation—an attempt at private ordering.[50] Thus, it was a change in the public's attitudes toward data collection in light of the new medium of the Internet that exerted pressure on the private sector, which ultimately culminated in regulation.[51] Despite the E.U.'s aggressive[52] stance toward data protection,

47 In fact, many of us advising clients at the time found ourselves wrestling with our consciences on a regular basis: we were divided between supporting the socially responsible action of urging our clients to disclose privacy practices, on the one hand, and, on the other, zealously representing our clients' interests to the logical end of advising them that privacy practices disclosures could only provide additional sources of liability within the United States.

48 *See* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 (2000); *see also* Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (1999).

49 *See* Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (1999).

50 For a discussion of private ordering in the context of regulation of the Internet, see Perritt, *supra* note 2, at 251–54.

51 Meanwhile, this insistence by clients on privacy policies, which clients believed to be necessitated by business reality, consequently resulted in a reaction by technology transactions counsel to assist our clients in minimizing negative legal repercussions to their chosen course of action. We moved to attempt to limit our clients' potential privacy liability and, simultaneously, to prevent their becoming subject to jurisdiction for privacy and other harms throughout the world, an onerous task in a constantly changing regulatory climate. Technology transactions counsel came to develop certain transactional Internet legal norms. These norms included such advice as urging clients to restructure database interoperability
in connection with Internet data; shifting contractual liability to other parties in Internet related contracts through, for example, choice of forum and law provisions and data privacy indemnifications; and including limitations of liability provisions in Terms and Conditions of Use with end users. Terms and Conditions of Use, which generally adopt the "everything but the kitchen sink" approach to contract drafting, are today a staple of websites, but were not omnipresent as recently as 1997. They masquerade behind such intriguing links as "Terms of Use," "A Note from our Lawyers," or "Legal." A majority of these agreements are unenforceable due to, among other reasons, their graphical user interface placement. For a discussion of enforceability of online terms and conditions of use, see *Specht v. Netscape Communications Corp.*, 306 F.3d 17 (2d Cir. 2002).

52 This stance was aggressive by U.S. standards, but certainly not by E.U. standards. In the European Union, the conception of an individual right to privacy differs from the conception of the right to privacy in the United States. Consequently, citizens and regulators approach questions of privacy from

the United States did not have any online consumer data protection legislation[53] in effect until April 2000.[54]
Therefore, it can be argued that the Internet has caused in part a social reconceptualization of the value of user data and, consequently, the role that privacy and personal information control play within our society and our regulatory structures.

B. Egalitarian Reconstruction of Corporate Identity

As correctly argued by Allan Stein, the common conception of corporate citizenship and, consequently, corporate identity has been mechanical.[55] Traditionally, a business entity has been perceived stereotypically to be a faceless behemoth, which conducts business and capitalizes on the commercial needs of individual consumers in various jurisdictions. As such, the idea of evolution of corporate citizenship and identity in jurisdictional context seems unthinkable. However, it can be argued that the Internet has resulted in two different identity convergence processes between individuals and business entities, which require that we begin to contemplate corporate identity in a developmental and evolutionary context. First, there is a convergence of personal, social, and collective identity into one medium. Second, and closely connected, there is a convergence in identity of sellers and consumers or, on the Web, content producers and users. Thus, I would argue that the constructs of corporate citizenship and individual citizenship are converging in light of the rise of Internet entrepreneurship.
Identity can be divided into at least three conceptually different types of identity: personal, social, and collective. Personal identity refers to construction of self as an atomized individual.[56] Social identity construction refers to ways that individuals construct their identity in relation to others, either as the sense of being an individual part of a group[57] or as a dynamic process in which the individual negotiates a desired identity.[58] Collective

a fundamentally different conceptual framework. The European Union approach may be characterized as one which begins from a presumption in favor of citizen privacy in commercial transactions, whereas the United States approach might be characterized as an approach that begins from a presumption against citizen privacy in commercial transactions. Though privacy guarantees in the United States and the European Union are slowly converging in favor of a regulatory approach closer to the position of the European Union, this movement is slow. *See* Steven R. Salbu, *The European Union Data Privacy Directive and International Relations*, 35 VAND. J. TRANSNAT'L L. 655, 691 (2002).

53 This statement does not contemplate any criminal statutes such as the Electronic Communications Privacy Act, 18 U.S.C. § 2701 (2000), which was passed in 1986.

54 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. § 312.

55 Stein, *Frontiers of Jurisdiction*, *supra* note 2, at 383.

56 *See, e.g.*, ERIK H. ERIKSON, CHILDHOOD AND SOCIETY 261 (1963); JEAN PIAGET & BARBEL INHELDER, THE PSYCHOLOGY OF THE CHILD 150 (2000).

57 *See, e.g.*, CYBERGHETTO OR CYBERTOPIA? RACE, CLASS, AND GENDER ON THE INTERNET (Bosah Ebo ed., 1998); Anita L. Allen, *Gender and Privacy in Cyberspace*, 52 STAN. L. REV. 1175, 1193 (2000); Jerry Kang, *Cyber-Race*, 113 HARV. L. REV. 1130, 1131 (2000).

58 ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 191 (1973).

identity is a sense of a responsibility for a group and an obligation to act as part of the group.[59]

The Internet blurred the lines among these three types of identity and, frequently, among commercial and noncommercial aspects of identity. It is impossible in many instances to ferret out the commercial and noncommercial aspects of Internet communications. Personal websites of individuals are interspersed among websites proposing bilateral commercial transactions and websites with interactive functions for groups such as bulletin boards and chatrooms, all of which may end up serving as a basis for both commercial and noncommercial exchanges. As such, all three types of identity building are possible using one medium, which, in theory at least, gives all speech equal voice.[60] The physical construct of content presentation on the Web, a website, is the same for all speakers, whether the speaker conducts business out of her garage or from her office as CEO of a multinational corporation. In this manner, all speech is equally valued. Similarly, the physical construct of content presentation does not discriminate on the basis of country of origin,[61] granting both users and content providers an international marketplace of ideas and products.

Along the same lines, the distinction between content production and content use has become increasingly eroded on the Internet as applications facilitate content production. This erosion has resulted in the function of content production and the function of content use being increasingly performed by the same individuals. As a consequence of this ease of content production, the Internet has enabled entrepreneurship to flourish online by eliminating at least one major barrier to market entry—overhead expenses associated with the use of physical space to market wares. Costs associated with physical overhead may have proven negatively dispositive for some

59 In connection with hacker collective identity, see, for example, STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION 39–50 (1984); E-mail from Timothy C. May, Crypto Anarchist Manifesto (Nov. 22, 1992), *available at* http://www.eff.org/Privacy/Crypto_misc/cryptoanarchist. manifesto; Eric Hughes, Cypherpunk Manifesto, *at* http://www.activism.net/cypherpunk/manifesto.html (last updated Mar. 3, 1993); Gregory B. Newby, The Hacker's Manifesto, The Conscience of a Hacker . . . by the Mentor . . ., *at* http://www.ils.unc.edu/gbnewby/code/archive/manifesto.html (last updated Jan. 8. 1986); Neal Stephenson, In the Beginning Was the Command Line, *at* www.cryptonomicon.com/beginning.html (last visited Nov. 8, 2003).

60 The same individual may have one website devoted to his online diary chronicling the personal angst of being the owner of an untrainable dog, be an online vendor of pet portraits through eBay (in an attempt to become the premiere dog portrait artist in the country), and run a schnauzer enthusiast bulletin board on a third website.

61 Granted, websites authored in languages foreign to the user will pose international barriers to comprehension. However, in light of plentiful translation tools online that are easily accessible through a search engine, even a language barrier may not be dispositive to understanding the message of the website's author. Similarly, if a government filters content accessible to its citizens, as the Chinese government does, the international voice of the medium becomes less potent. For a discussion of China's filtering of the Internet "pipe," see Panel Discussion with Shanthi Kalathil, James Mulvenon & Benjamin Edelmen, China and the Internet: A New Revolution? (Mar. 14, 2003) (moderated by Minxin Pei) (summary of event at http://www.ceip.org/files/events/events.asp?EventID=595).

entrepreneurs; however, through virtual storefronts, such entrepreneurs have been empowered to include economic self-realization as an element of their social identity construction, both as individuals and as stakeholders in a business entity.[62] Also, because of the immediacy of a large global audience provided by the Internet and the intermediation of services such as eBay, commerce for entrepreneurs shifted from being a small local enterprise to an instantly global operation, sometimes with a significantly larger audience.[63]

Therefore, as the Internet has blurred both the lines among personal, social, and collective identity and the lines between corporate-content producer and individual consumer, the time is ripe to reevaluate an overly simplified construction of corporate citizenship. As a consequence, the way that we conceptualize the relationship between corporate entities and states should shift in favor of a consensual model of social responsibility; just as individual citizens of a state accept responsibility for the organization and socio-political agenda of a state through elections of officials, so business entities can and should accept social responsibility for maintenance of the trusted system of economic exchange within the state.

C. How the Shift in Economic Identity Impacts Jurisdiction

The shift in economic identity described in the preceding section involves two of the primary differences between the manner in which exchanges of information occur using Network Communications and the manner in which they occur in physical space—the extent of data collection and the egalitarian presentation of all content providers. Both of these differences fundamentally describe types of information dissymmetry between the content provider and the content user that do not occur in real space. In real space, if an individual enters a bookstore and picks up a copy of a newspaper to read the headline, little or no systematic information collection occurs about the individual unless he or she purchases the paper (and then usually only if the consumer uses consideration other than cash). On the Web, however, the likelihood of extensive information collection by both the physical structure containing the newspaper (the website) and the newspaper itself (certain pages within the website) is greatly increased. Similarly, many of the external cues of credibility upon which individuals rely in real space are either absent or differently operationalized. For example, whereas a user may never walk into a bookstore that has a certain

[62] Frequently, social identity building can involve an element of economic self-realization, involving both a quest for professional attainment and an element of commercial exchange. The transaction costs of virtual storefronts are in large part limited to fees associated with a limited number of information production and maintenance relationships, such as content development and hosting.

[63] For example, it is highly unlikely that I, a Chicagoan, would have purchased Hebridean toffee from the Island of Barra were it not for an Internet presence of the toffee vendor at http://www.isleofbarra.com and the intermediation of Google.

distant physical location and read a newspaper, a user may, without hesitation, visit an unknown website that hosts a newspaper, which the user may have found as a consequence of an imperfect search result from a search engine.[64] The informational terms on which actors engage are fundamentally altered in the context of Network Communications. A qualitatively different relationship exists between information conveyed by the content provider and the content user in real space and in virtual space.[65] Although not articulated by courts in the above manner, it was these inequities in information that have resulted in analytical difficulties for courts in the context of Internet jurisdiction determinations. Not long after the launch of the Mosaic browser,[66] courts became embroiled with the initial wave of litigation arising out of the burgeoning medium of the Internet.[67] Courts recognized early on that, although the jurisdictional inquiry in Internet-related cases was similar to all other jurisdictional inquiries, certain properties of the medium complicated the calculus.[68] The dynamics of content providers and users were somehow different.

The most obvious of these complicating properties, which was repeatedly noted by courts, is the global omnipresence of connectivity presented by the Internet. Anyone anywhere in the world theoretically could view a website.[69] Courts have struggled heartily with the issue of Internet contacts and assertions of jurisdiction. In general, the approaches of courts to jurisdictional inquiries in cases involving significant Internet contacts can be divided into two different types: (1) Internet-specific approaches, which include a blanket approach (represented by *Inset Systems, Inc. v. Instruction Set, Inc.*[70]) and a sliding scale approach (which was set forth in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*[71]) and (2) a traditional jurisdictional approach or modified sliding scale approach, usually relying on *Calder v. Jones*.

64 For instance, the likelihood that I would ever walk into a local bookstore in Great Falls, Montana to read the classified advertisements in connection with non-traditional livestock in the Livestock Roundup section of the THE PRARIE STAR is very low (assuming I know the paper exists at all) because I have no real need to keep abreast of the nontraditional livestock market. On the Web, I, without hesitation thanks to Google's creative intermediation, will allocate two minutes to peruse the panoply of nontraditional livestock options available to me in the greater Great Falls, Montana area. *See* Livestock Roundup, http://www.livestockroundup.net/classifieds/index.inn?loc=sub&main=Livestock.

65 For a discussion of the different impact of online and offline environments on building customer trust, see Sirrka L. Jarvenpaa & Emerson H. Tiller, *Customer Trust in Virtual Environments: A Managerial Perspective*, 81 B.U. L. REV. 665 (2001).

66 Mosaic was developed in 1993. *See supra* note 38.

67 *See, e.g.*, Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996), Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997).

68 *See, e.g.*, cases cited *supra* note 67.

69 *See Zippo*, 952 F. Supp. at 1123; GTE New Media Servs., Inc. v. BellSouth Corp., 199 F.3d 1343, 1350 (D.C. Cir. 2000).

70 937 F. Supp. 161 (D. Conn. 1996).

71 952 F. Supp. 1119 (W.D. Pa. 1997).

1. Cases Representing Internet-Specific Approaches.—Two types of Internet-specific standards have arisen in the course of courts' jurisdictional inquiries in cases with facts related to the Internet. The first is an approach represented by *Inset v. Instruction Set, Inc.*, which stands for the proposition that simply by launching a website, a content provider consents to jurisdiction in every jurisdiction worldwide where the website can be viewed. Essentially, under *Inset*, a website's being live equals consent to jurisdiction.
The second Internet-specific approach, a sliding scale approach, arose out of *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.* This sliding scale approach turns on the perceived interactivity of the graphical user interface or "GUI" of a website from a user's perspective, with "passive" websites representing inadequate basis for jurisdiction and fully "interactive" websites automatically triggering jurisdiction in all jurisdictions.

a. Inset Systems, Inc. v. Instruction Set, Inc.—One of the first cases to address jurisdiction in the context of the Internet was *Inset Systems, Inc. v. Instruction Set, Inc.* In this case, the jurisdictional inquiry turned on whether a defendant-operated website, which contained a toll-free number for contacting the company and advertising for its products, provided adequate basis for personal jurisdiction over the defendant.[72] The Connecticut district court found that personal jurisdiction over the defendant existed in Connecticut based on the defendant's website.[73] Because any Connecticut resident could access the website, Inset had made contacts that constituted sufficient minimum contact for purposes of due process.[74] In general, courts view the *Inset* decision unfavorably and disregard its analysis.[75] It has come to stand for the idea that mere access to a defendant's website presents adequate minimum contacts with a forum to sustain jurisdiction.[76]

Although the rationale proffered by the court in *Inset* was flawed in some respects, as will be explained subsequently in this Article, summarily disregarding *Inset*'s analysis is unwarranted and, perhaps, inadequately contemplative of the types of harms that arise from contacts involving websites. The outcome in *Inset*, based on a different rationale grounded in a minimum contacts analysis, may have been appropriate. *Inset*'s value arises primarily in the legal, but technologically-driven question it pushes us to ask: Can, today or in the future, a "tombstone"[77] website or other seemingly passive

72 *Id.* at 164.
73 *Id.* at 165.
74 *Id*.
75 *See, e.g.*, Envisionet Computer Servs. v. Microportal.com, Inc., No. 00-225-P, 2001 WL 179882, at *6 (D. Me. Feb. 14, 2001).
76 *Id.*
77 I am using the term "tombstone" in a manner similar to that used in securities regulations. In the securities context, a tombstone advertisement is an advertisement that contains very basic information about an upcoming offering, primarily only the name of the issuer, the class of securities, and the amount of the issue. For a discussion of tombstone advertisements in securities regulation, see Michael

Network Communication cause harm and sufficient minimum contacts through its mere accessibility within a forum?[78] It was in the context of this question that the sliding scale approach arose. Unfortunately, however, the sliding scale approach ultimately answered the question erroneously.

b. Zippo Manufacturing Co. v. Zippo Dot Com, Inc.—In *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, a Pennsylvania district court embarked on a reexamination of the approach adopted by the *Inset* court. It set forth a sliding scale approach that disagreed with the analytical framework adopted by the *Inset* court.[79] The *Zippo* court's "sliding scale" approach presented a tripartite analytical framework based around website "interactivity"[80] and implicitly structured from the user's perspective. If, presumably from a user's perception of the website's GUI on its face, the website is a "passive [w]eb site"[81] that only functions to make information available to users in any jurisdiction, the sliding scale approach would indicate that jurisdiction in a forum other than the content provider's forum would be unsustainable. The next category of the sliding scale approach addresses websites that fall into a cavernous gray area of "interactive [w]eb sites where a user can exchange information with the host computer."[82] With regard to such websites, the *Zippo* court stated that "the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the [w]eb site."[83] Finally, the third part of the Zippo sliding approach applies to websites that conduct full e-commerce activities, meaning that an entire purchase of a product occurs online. Such websites are subject to jurisdiction everywhere because of the nature of the website.[84]

Numerous courts have cited to and applied the sliding scale approach; for better or worse, it is now considered the primary framework for analysis of an Internet jurisdiction inquiry.[85] However, the analytical efficacy of the sliding scale is small, and numerous other courts have felt the need to supplement the potency of the sliding scale approach.

86 E. Schoeman, *The First Amendment and Restrictions on Advertising of Securities Under the Securities Act of 1933*, 41 BUS. LAW. 377, 379 (1986).

78 Despite *Inset*'s outcome, even assuming that an entrepreneur wanted to comply with the law of every jurisdiction where the website was viewable, the legal costs of ascertaining what the law required in each jurisdiction would prove prohibitive.

79 *Zippo*, 952 F. Supp. at 1123–24.

80 *Id.* at 1124.

81 *Id.*

82 *Id.*

83 *Id.*

84 *Id.*

85 *See, e.g.*, Kovacs v. Jim, No. 02C7020, 2002 WL 31507172, at *2 (N.D. Ill. Nov. 12, 2002) ("[M]ost courts look to the 'sliding scale' framework established by *Zippo* . . . .").

86 Revell v. Lidov, 317 F.3d 467, 471 (5th Cir. 2002).

While we deployed this sliding scale in *Mink v. AAAA Development LLC,* it is not well adapted to

2. The Shortcomings of Current Technology-Specific Approaches.—Current Internet jurisdiction standards are a morass of inconsistent case law with dubious precedential value. Similarly, the Internet jurisdiction scholarship represents a lack of consensus, but for the uniform acknowledgement of inconsistency in case law. Internet-specific standards that are not rooted in traditional jurisdictional approaches do not provide optimal approaches toward building a sustainable framework for Internet jurisdiction determinations. Internet-specific approaches explored to date tend to fall short on both technological and social policy grounds, frequently resulting in unpredictable outcomes. Such approaches will hinder the achievement of an international consensus on reciprocal standards for assertions of jurisdiction and recognition of judgments.

On technological grounds, current "Internet" specific approaches are inadequately neutral. Without acknowledging it, they revolve around one particular incarnation of Network Communications, the World Wide Web, in a technologically stagnant manner. As such they are destined for a short shelflife; they do not provide sufficient intellectual flexibility for use with the next generation of Network Communications. This type of rigidity poses particular concerns in a precedent-based common law system. In the context of broader U.S. social policy, technology-specific regulatory approaches fail to strike a successful balance between incentivizing Internet entrepreneurship and redressing harms arising out of such entrepreneurial ventures. They also fail to acknowledge the inevitability of E.U.-U.S. Internet regulatory convergence.

Finally, Internet-specific jurisdictional frameworks currently in use, most notably the sliding scale approach, clearly bear the time-date stamp of the state of the law at the particular moment in technology history in which they were constructed. Consequently, their usefulness is limited.

a. Lack of technology neutrality.—According to Moore's[87] law,[88] the number of transistors in integrated circuits is doubling approximately every eighteen months, though some evidence indicates the rate has slowed to every twenty-four months.[89] This statistic provides an example of

the general jurisdiction inquiry, because even repeated contacts with forum residents by a foreign defendant may not constitute the requisite substantial, continuous and systematic contacts required for a finding of general jurisdiction—in other words, while it may be doing business *with* Texas, it is not doing business *in* Texas. *Id.*

87 Gordon E. Moore cofounded Intel Corporation. *See* Press Release, Haas School of Business, Univ. of California, Berkeley, Intel Founder Gordon Moore Receives Lifetime Achievement Award at Haas/UC Berkeley's Entrepreneurship Center (May 2, 2000), *available at* http://www.haas.berkeley.edu/groups/pubs/news/articles/gmoore050200_.html.

88 Gordon E. Moore, *Cramming More Components onto Integrated Circuits*, ELECTRONICS, Apr. 19, 1965, ftp://download.intel.com/research/silicon/moorespaper.pdf; *see also* CNet Glossary: Moore's Law, *at* http://www.cnet.com/Resources/Info/Glossary/Terms/mooreslaw.html; Intel Corp., Silicon: Moore's Law, *at* http://www.intel.com/research/silicon/mooreslaw.htm.

89 Mark D. Hill, Harnessing Moore's Law, *at* http://www.cs.wisc.edu/~cs354-1/cs354/handouts/markhill_moore_01_09.pdf (last updated Aug. 2001).

the stunning pace of technological evolution. The expansion of technological capabilities of applications, as well as hardware, is similarly impressive. In 1997, the year *Zippo* was decided, approximately 93.7 million email accounts existed; that number is projected to rise to 187 million by 2014.[90] The role that Network Communications play in our society is burgeoning and is not contingent on the technology "bust" of 2001. U.S. citizens are using Network Communications in record numbers, and they are conducting commerce over these networks. Business to consumer e-commerce activity continues to increase.[91]

From the outset, definitionally speaking, an odd lexical problem exists: current "Internet jurisdiction" frameworks are not really about the Internet.[92] They are actually structured to revolve around issues that arise on the World Wide Web. This misnomer presents a substantial problem for future jurisdictional inquiry. Specifically, an interesting dichotomy has arisen in jurisdictional determinations: email contacts frequently are treated by courts as telephone contacts for jurisdictional purposes,[93] while websites are subject to a different "Internet" framework, usually the sliding scale approach. For example, in *Verizon Online Services, Inc. v. Ralsky*,[94] a spammer objected to jurisdiction in connection with a suit against him for sending millions of unsolicited bulk emails to users of an Internet service provider. In that case,

90 Gary E. Machlis et al., A Look Ahead: Key Social and Environmental Forecasts Relevant to the National Park Service 24, http://www.nps.gov/socialscience/waso/A_Look_Ahead.pdf (last updated Sept. 2000).

91 Lisa Gill, *Study: Consumers Plan More Online Spending in 2003*, ECT NEWS, Jan. 20, 2003, *at* http://www.ectnews.com/perl/story/20512.html.

92 Use of the World Wide Web represents only a portion of Internet activities. The Internet includes communications not using the World Wide Web and websites. For example, email, Usenet, and various information relay applications use the Internet, but are not Web-based applications. For a discussion of the difference between the Internet and the World Wide Web, see Tim Berners-Lee, Press FAQ, *at* http://www.w3.org/People/Berners-Lee/FAQ.html (last visited Oct. 24, 2003); Webopedia, The Difference Between the Internet and the World Wide Web, *at* http://www.webopedia.com/DidYouKnow/Internet/2002/Web_vs_Internet.asp (last visited Nov. 8, 2003); United States v. Am. Library Ass'n, Inc., 123 S. Ct. 2297, 2310 (2003) (Breyer, J., concurring) (describing the Internet as a "vast democratic" medium and the World Wide Web, in part, as "comparable, from the readers' viewpoint, to . . . a vast library" (citing Reno v. ACLU, 521 U.S. 844, 853, 868 (1997))).

93 *See, e.g.*, Verizon Online Servs., Inc. v. Ralsky, 203 F. Supp. 2d 601, 615 (E.D. Va. 2002) ("[I]n contrast to an Internet Web site, 'the active as opposed to passive nature of e-mail weighs in favor of finding personal jurisdiction in the forum where the e-mail is received.'" (quoting Internet Doorway, Inc. v. Parks, 138 F. Supp. 2d, 773, 777 (S.D. Miss. 2001))); Machulsky v. Hall, 210 F. Supp. 2d 531, 539 (D.N.J. 2002) ("[E]mail communications must occur within the context of other 'substantial' connections to the forum in order to constitute purposeful availment . . . ."); Reliance Nat'l Indem. Co. v. Pinnacle Cas. Assur. Corp., 160 F. Supp. 2d 1327, 1333 (M.D. Ala. 2001) ("E-mails, like letters and phone calls, can constitute minimum contacts, at least if the defendant or his agents send the message for pecuniary gain rather than substantially personal purposes."); Phat Fashions, L.L.C. v. Phat Game Athletic Apparel, Inc., 00 Civ. 0201, 2001 U.S. Dist. LEXIS 13892, at *11 (S.D.N.Y. Sept. 7, 2001) ("Mere telephone, mail, or e-mail contacts will normally not suffice to support jurisdiction . . . .").

94 203 F. Supp. 2d at 601.

unlike many other cases addressing email contacts,[95] the court struggled to find a way to apply the sliding scale approach to the context of email. Finally, the court settled on interpreting *Zippo* to stand for the proposition that the "commercial nature of the exchange of information between a Web site and visitors [is a] possible basis for exercising personal jurisdiction,"[96] but supplemented this analysis with additional frameworks. Both email and websites pose essentially the same questions regarding Network Communications, particularly with regard to privacy and security harms. For example, an email commonly is authored using hypertext markup language ("HTML"),[97] one of the languages used to write websites.[98] Consequently, emails in HTML present the same type of concerns that a website in HTML would present as a live data feed connecting to a user's central processing unit—regardless of whether the content of the email is commercial or noncommercial in nature.[99] The HTML message sent to the recipient is, in actuality, only a live shell that points to Internet content. In this manner, the distinction between content arriving in an email or being live somewhere on the Web becomes unsustainable.[100] This example points to, perhaps, the critical technological gaffe in current Internet jurisdiction case law—technological over-determinism.

A regulatory lesson that has been repeatedly learned through trial and error, most recently by the European Union in the context of Internet data privacy regulation,[101] is that a delicate balance exists between, on the one hand, adequate technological specificity in regulation to allow for compliance and, on the other, maintaining adequate technology neutrality to allow for an extended regulatory shelf-life. Striking this balance is difficult, but

95 *See supra* note 93.
96 *Verizon*, 203 F. Supp. 2d at 614.
97 HTML is discussed in W3C, Hypertext Markup Language, *at* http://www.w3.org/MarkUp/.
98 Markup Languages, *at* http://webreference.com/authoring/languages/ (last modified July 28, 2000).
99 *See, e.g.*, Stefanie Olsen, *Nearly Undetectable Tracking Device Raises Concern*, CNET NEWS.COM, *at* http://news.com.com/2100-1017-243077.html?legacy=cnet (last modified July 12, 2000); *Virus Writers Turn to Spam*, BBC NEWS, *at* http://news.bbc.co.uk/2/hi/technology/3107613.stm (last modified July 30, 2003) ("'Clicking on a link in a spam e-mail is the equivalent of handing a burglar the keys to your house.'").
100 In the words of one cryptography expert, HTML email is used for one or more of three purposes: "righteous" (reducing traffic by sending a link instead of a large image), "nefarious" (tracking the recipient), and "dubious" (allegedly for additional security reasons). E-mail from Cem Paya, Senior Program Manager, Microsoft Corporation, to Andrea Matwyshyn, Clinical Assistant Professor of Law, Northwestern University (Oct. 15, 2003) (on file with author).
101 The most recent E.U. E-commerce Directive, Council Directive 2002/58, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) 2002 O.J. (L 201/37), *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf, was specifically enacted to remedy the technological over-determinism of previous directives. It explicitly repeals Council Directive 97/66, 1997 Privacy Protection Telecommunication Sector 1997 O.J. (L. 201/37) for this reason.

Internet-specific jurisdictional frameworks, at least the ones proposed to date, fail to plan for the inevitability of technological convergence and evolution into new forms of Network Communications. The courts have crafted a jurisdictional standard based on websites, a particular manifestation of Network Communications. Instead, a more successful approach may be to more broadly craft standards that address the nature of the data flows and the ways harms arise as a consequence of data flows through Network Communications, regardless of the particular technological manifestation or structure of the communication network.

b. Lack of consideration of data harms.—Perhaps the clearest illustration of the conceptual shortcomings of current Internet jurisdiction frameworks arises in cases addressing potential data privacy and security related harms. Content providers have become and will continue to become increasingly adept at latent data collection. Moreover, as data collection and processing is increasingly outsourced to third-party providers,[102] users' ability to determine the data collection processes occurring in connection with their Network Communications will require increasing degrees of technological sophistication. Because the primary means of data collection disclosure will be provided by the entity conducting the data collection, many unscrupulous entities will misrepresent the data collection practices occurring, for example, on a website, and subsequently breach those privacy promises.

Although some cases seeking redress for technology-related data privacy harms will be presented in the form of breach of contract actions based on entities' stated privacy policies, a portion of these cases, like *In re Pharmatrak, Inc.*,[103] will not. The facts of *Pharmatrak* serve as a useful illustration of the types of harms that will continue to occur in connection with Network Communications. They also demonstrate the problems presented for current Internet jurisdiction frameworks in connection with data farms.

In *Pharmatrak*, a third-party provider of hosting services under contract with several pharmaceutical companies collected personally identifiable user information regarding user searches. The actions of the thirdparty provider were in express breach of the terms of the outsourcing agreement. Users sued both the third-party provider, Pharmatrak, Inc., and the pharmaceutical companies for violation of the Electronic Communications Privacy Act.[104] The Court of Appeals for the Fifth Circuit reversed an order of summary judgment against a class of Internet users harmed by Pharmatrak's breach. It also found against Pharmatrak, Inc., stating that

[102] This business reality is reflected, for example, in the Gramm-Leach-Bliley Act, which includes particular contractual restrictions that "financial institutions" must impose on third-party data processors. *See* 15 U.S.C. §§ 6801-6809 (2000).
[103] 329 F.3d 9 (5th Cir. 2003).
[104] *Id.* at 12.

neither the pharmaceutical companies nor the consumers consented to the interception of personal information by Pharmatrak Inc. that occurred during users' use of the websites at issue. The websites in question used cookies,[105] web bugs,[106] and the "get" method[107] of information retrieval and accumulated information on users, including names, addresses, telephone numbers, email addresses, birthdays, sex, insurance information, educational information, income, occupations, medical conditions, current medications, reasons for visiting the website, and even the subject, sender, and date of the web-based email messages that users were reading immediately prior to visiting the websites of Pharmatrak clients.[108] Although perhaps some more sophisticated users may have noticed the get method being used in lieu of the post method[109] on the websites in question or realized a web bug was being used on them and a subsequent cookie dropped, it is highly unlikely that a reasonable user had an adequate degree of technological sophistication to recognize the data collection processes at work. Instead, a reasonable user would have looked to the posted privacy policy on the website he or she was visiting. Pharmatrak's breach of the contractual terms of its services resulted in a corollary breach of the contractual terms of the privacy policies posted on the implicated websites.

As demonstrated by the facts of *Pharmatrak*, websites that a user perceives to be simply "dead advertising" or content that is not collecting significant amounts of information and thus deemed to be relatively "passive" under the sliding scale approach[110] may, in fact, be still highly interactive in real terms because of the extent of data collection being conducted in relation to the user. When most users look at a website, they can never be certain whether surreptitious data collection is occurring; they are forced to rely on a data practices disclosure provided by the website. Comparatively, an operator of a billboard in real space does not have the capability to know anything about its onlookers unless the billboard has an implanted camera. An offline newspaper advertisement does not send back pageview information informing the publisher or advertiser of the amount of time a reader spent looking at a particular advertisement, whether the reader quickly turned the page in disgust, and what the reader picked up subsequent to the

105 A cookie is a small text file that a website writes to a user's hard drive in order to recognize the user either during the user's session on a website (a session cookie) or during subsequent visits to the website (a permanent cookie). *See, e.g.*, Ask Bruce, BBC, *at* http://www.bbc.co.uk/webwise/askbruce/articles/browse/cookie_1.shtml.

106 Web bugs are discussed *supra* note 17.

107 The "get" method of information retrieval is generally not used for sensitive user data collection because the entered information becomes included in the URL generated subsequent to the user's entry of the information. *In re Pharmatrak*, 329 F.3d at 14.

108 *Id.* at 15.

109 The "post" method of data collection, unlike the "get" method, does not display information input by the user in URLs and provides a more secure method of data entry and conveyance. *Id.* at 16.

110 Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997).

newspaper.[111] As such, the *Inset* court was not completely wrong—it is possible that the mere accessing of a website that is not fully "interactive" by sliding scale standards[112] could create sufficient harm to warrant jurisdiction.[113]

c. Disincentives for entrepreneurship.—Neither the *Inset* approach, nor the *Zippo* sliding scale approach successfully strike a balance between stimulating intellectual entrepreneurship in Internet-content production and obtaining redress for harm resulting from Internetentrepreneurial ventures. The *Inset* approach strongly disincentivizes Internet entrepreneurship; by merely launching a website of any kind, an entrepreneur exposes herself to lawsuits in every jurisdiction. *Inset* presumes that a content provider is always in a better position to bear costs of litigation and that systemic protections against subjecting content providers to frivolous suit are superfluous.[114]

The sliding scale approach similarly disincentivizes entrepreneurship in content production. Theoretically, any newspaper website that facilitates intellectual discourse, for example, through providing interactive bulletin boards for users or real time debate with columnists,[115] would fall either into the middle gray area in the sliding scale[116] or in the interactive area, which automatically triggers jurisdiction. The treatment of this vast gray area in the sliding scale approach cannot be predicted consistently. Thus, for all practical purposes, the *Inset* and sliding scale approaches both present strong disincentives to Internet entrepreneurship.

3. Cases Representing a Traditional or Modified Zippo *Jurisdictional Approach Rooted in* Calder v. Jones.— An increasing number of recent cases remind us that, regardless of the medium through which a claim arises, on the most fundamental legal level, all jurisdictional inquiries must be conducted in a manner consistent with the Due Process Clause. Simultaneously, however, many of the cases that rely on traditional jurisdictional principles in lieu of, or in addition to, a sliding scale approach, often adopt a

111 Web bugs have the capability to follow a user onto websites after the original website and, in some instances, even read web-based email messages the user reads. *See, e.g.*, Electronic Frontier Foundation, The Web Bug FAQ, *at* http://www.eff.org/Privacy/Marketing/web_bug.html.
112 *Zippo*, 952 F. Supp. at 1124.
113 The *Inset* court analogized Inset's creation of a website to the purposeful placement of advertisements in Connecticut papers. Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161, 164 (D. Conn. 1996). This analogy, based on the facts offered in the *Inset* decision, was not supportable. However, had the *Inset* court researched the number of residents of the state of Connecticut who actually saw the website and analogized this number to the number of subscribers who would have viewed the content had it been placed in a newspaper, the court would have crafted a stronger argument for an assertion of jurisdiction on the basis of a targeting rationale.
114 However, the *Inset* approach is not completely in error: a "passive" website under the sliding scale approach can still cause harm and should, in some instances, be an adequate basis for jurisdiction.
115 This would be the case even if no commercial transactions were carried out online.
116 *Zippo*, 952 F. Supp. at 1124.

version of the "effects test"[117] set forth in *Calder v. Jones*[118] or a targeting approach intellectually rooted in *Calder*.

For example, in *Panavision International, L.P. v. Toeppen*,[119] the Ninth Circuit addressed whether the California district court properly asserted jurisdiction over a cybersquatter who did not reside within the forum, but had registered a domain name using the trademarks of a legal person within California.[120] Although the decision in Panavision cites to *Zippo*,[121] the rationale articulated by the Ninth Circuit is one based in a traditional minimum contacts analysis. In other words, the defendant needs to have had sufficient contacts with the forum, such that "maintenance of the suit does not offend traditional notions of fair play and substantial justice"[122] and the defendant could have reasonably anticipated being haled into court[123] in that forum. The defendant's websites with the offending uniform resource locators were "passive;" one had posted pictures of a town in Illinois, and the second merely had the word "Hello" typed across the GUI. By using a sliding scale approach, no basis for jurisdiction would have been found due to the lack of interactivity of the websites at issue. However, instead of strictly applying the sliding scale, the Ninth Circuit applied the "effects test" set forth by the Supreme Court in *Calder*.[124] The Ninth Circuit found that the defendant intended to cause harm to a California resident, Panavision, and was aware that the effects of the tortious action would be felt in California.[125] Similarly, the Fourth and Seventh circuits have conducted a jurisdictional analysis reflecting an approach based, in varying degrees, on the "effects test" articulated in *Calder*.[126]

In other instances, however, courts have not applied the sliding scale approach even in part; instead, applying traditional jurisdiction principles,

117 The effects test adopted in *Calder v. Jones*, 465 U.S. 783, 787 (1985), assesses whether a defendant knew or should have known that a plaintiff in a particular forum would feel the effects of the defendant's actions. As set forth by one court, the elements of a *Calder* analysis are: (1) the defendant must commit an intentional tort; (2) the plaintiff must feel the brunt of the harm in the forum such that the forum can be said to be the focal point of the harm suffered by plaintiff as a result of the tort; and, (3) the defendant must expressly aim his or her tortious conduct at the forum so that the forum can be said to be the focal point of the tortious activity. Barrett v. Catacombs Press, 44 F. Supp. 2d 717, 730 (E.D. Pa. 1999).
118 465 U.S. at 783.
119 141 F.3d 1316 (9th Cir. 1998).
120 *Id.* at 1319.
121 *Id.* at 1320.
122 *Id.* at 1322.
123 *Id.* at 1320.
124 *Id.* at 1321.
125 *But see* Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414, 418 (9th Cir. 1997) (finding that foreign defendant's advertisements on website were not adequate to find personal jurisdiction and stating that "something more" than mere publication is required, in line with J. O'Connor's plurality opinion in *Asahi Metal Industries Co. v. Superior Court*, 480 U.S. 102, 112 (1992)).
126 465 U.S. 783 (1984).

they construed users' access of a website to constitute third-party action that does not give rise to jurisdiction over the defendant. For example, in *GTE New Media Services, Inc. v. BellSouth Corp.*,[127] the D.C. Circuit did not affirm the lower court's application of the sliding scale approach and, thus, may have called the viability of the sliding scale approach into question.[128] In the dispute, the defendants operated websites from which users could obtain telephone numbers in an online "Yellow Pages."[129] The websites at issue were clearly interactive and commercial in terms of the sliding scale approach. As such, the sliding scale approach mandated that jurisdiction be upheld. However, the D.C. Circuit chose not to apply the sliding scale approach and stated that despite the highly interactive nature of the defendants' websites, the activities of users did not amount to transacting business with the defendants. Therefore, jurisdiction was not supportable because the use of the website constituted unilateral acts by D.C. residents and not online transactions.[130]

4. The Shortcomings of a Traditional or Modified Zippo *Jurisdictional Approach Rooted in* Calder v. Jones.—Perhaps the strongest proponent of a "targeting" test for Internet jurisdiction is Professor Geist. He correctly argues that the *Zippo* test is ill-suited for the future of Internet jurisdiction inquiry and asserts that *Zippo* is based in a traditional jurisdictional analysis premised on foreseeability.[131] However, he rejects a jurisdictional approach grounded in traditional jurisdictional analysis for determinations of jurisdiction arising from Internet contacts.[132] Instead, he argues for a three-factor, Internet-specific targeting test involving contracts, technology, and actual or implied knowledge, with no single factor being determinative.[133] The approach evaluates the preexisting contractual relationship. In particular, it considers any forum selection clauses that were included in contracts; the use of and knowledge obtained from geolocation technologies; and additional knowledge obtained from activities, such as filling orders, financial records, and traffic monitoring.

Professor Geist's targeting approach correctly identifies the three component parts of controlling claim creation on the Web and, thus, contributes meaningfully to the discourse. However, the approach he advocates is less

127 199 F.3d 1343 (D.C. Cir. 2000).
128 *Id.*
129 *Id.* at 1346.
130 *Id.* at 1350.
131 "It must also be remembered that the *Zippo* passive versus active test was grounded in traditional jurisdictional principles. The analysis conducted as part of the test draws heavily from a foreseeability perspective." Geist, *supra* note 2, at 1371.
132 "Given the inadequacies of the *Zippo* passive versus active test, it is now fitting to identify a more effective standard for determining when it is appropriate to assert jurisdiction in cases involving predominantly Internet-based contacts." *Id.* at 1345.
133 *Id.* at 1384–1404.

than fully effective for two reasons. First, despite attempting to differentiate itself from the "effects test" articulated in *Calder v. Jones*, the targeting approach is grounded in a "focal point" analysis like that used in *Calder*.[134] As argued by leading jurisdiction scholars,[135] *Calder* is a fatally-flawed jurisdictional precedent; reliance upon it weakens the potency of any approach. Intellectually grounding any jurisdictional approach for addressing the unique problems posed by Network Communications in a precedent that is aberrant from the rest of jurisdiction case law limits the likelihood of longevity. The approach, assuming it is at least in part the correct approach, needs to be regrounded in the language of the rest of jurisdiction case law in lieu of *Calder*, an inexplicable outlier case. The approach advocated by Geist also provides no substantive guidance for the implementation of an effects/targeting approach. Therefore, the effects/targeting approach is left completely vulnerable to the inherent circularity of reasoning in the *Calder* jurisdictional approach. Second, a targeting approach is basically a rationalization of the unilateral exercise of control by a state at its discretion; it does not provide adequate guidance for online actors attempting to limit liability, particularly entrepreneurs providing "noninteractive" content, such as a newspaper. Thus, an effects/targeting approach to jurisdiction is inherently unfriendly to entrepreneurship. Finally, despite advocating technology neutrality, Professor Geist's approach is not technologically neutral, and it wrongly dismisses a regime of jurisdiction information based on self-disclosure. The approach advocates a jurisdictional regime that de facto legally mandates the use of increasingly more invasive and still imperfect "high tech," means such as geolocation,[136] over the "low tech" solution of self-disclosure. In this manner, the approach sets a high standard that puts cash-poor entrepreneurs at a disadvantage. A jurisdictional approach implemented from a "low tech" starting point of self-disclosure with the option, but not the requirement, of volitional supplementation with other technology is an approach more sensitive to the needs of entrepreneurs.

a. The problems of Calder *and its derivatives*.—Stretching the precedent of *Calder* as an intellectual grounding to accommodate claims arising out of Network Communications contacts is a tenuous rationalization for a jurisdictional approach. *Calder*'s theoretical underpinnings pre-

134 In fact, to justify his approach, Professor Geist indirectly cites to *Calder* by citing to Bancroft & Masters, Inc. v. Augusta National Inc., 223 F.3d 1082, 1087 (9th Cir. 2000), which cites to *Calder*. Geist, *supra* note 2, at 1381.

135 *See, e.g.*, Redish, *supra* note 2, at 596–600.

136 Geolocation is a service that geographically places in physical space the unique identifier of an individual surfing the Web with a high, but not perfect, degree of accuracy. Such services are provided either by a third-party service provider on an outsourced basis or are connected to internal networks through an application service provider arrangement on an in-house installation basis within the boundaries of the datacenter, even if licensed from elsewhere. *See, e.g.*, Meta Group, *Perils, Promises of Geolocation*, CNET NEWS.COM, *at* http://news.com.com/2009-1023-256139.html?legacy=cnet (Apr. 19, 2001).

sent an approach to jurisdiction that is out of line with all other constitutional precedent that explicitly rejected[137] this mode of analysis, an intellectual inconsistency that the *Calder* decision does not explain.[138] The *Calder* effects test and the subsequent effects/targeting approaches to jurisdiction are out of line with all other jurisdictional precedent in both analytical level and structure of argumentation. Borrowing an analytical framework from Bronfenbrenner,[139] it might be said that all constitutional jurisdiction case law outside of *Calder* focuses its attention primarily on macrosystem[140] analytical factors, meaning the interest of the state in asserting jurisdiction, and microsystem[141] analytical factors, the effect of finding jurisdiction on the defendant's rights.[142] Jurisdiction determinations, outside of *Calder*, inherently balance the rights of states in asserting control over a defendant against the defendant's liberty interests in being free of such control.[143] A *Calder* effects test and a derivative targeting approach, conversely, conduct an analysis solely on the mesosystem[144] analytical level. *Calder* looks to the particular claim at issue and addresses only the relationship between the defendant and the plaintiff, without first addressing the defendant's independent relationship to the forum. As such, *Calder*'s analysis is circular in its reasoning.[145]

137 *See* Hanson v. Denckla, 357 U.S. 235, 253 (1958).
138 *See* Calder v. Jones, 465 U.S. 783, 783 (1984).
139 URIE BRONFENBRENNER, THE ECOLOGY OF HUMAN DEVELOPMENT (1979).
140 Macrosystem level analysis requires examination at the level of culture as a whole, along with belief systems and ideologies underlying cultural rules and norms. In other words, the analysis focuses on the mechanisms of social governance and the worldview prevalent in civil society. *Id.* at 258.
141 On the microsystem level, individuals and their psychological development in a particular context is the primary level of analysis. *Id.* at 109.
142 *See, e.g.*, Int'l Shoe Co. v. Washington, 326 U.S. 310 (1945).
143 Thus, the specific jurisdiction inquiry proceeds in the following manner: A (the defendant) engages in certain conduct involving B (the state); B has a resident, C (the plaintiff), who alleges that he or she has been harmed by A. Therefore, jurisdiction over A is proper if it does not offend due process and claim C □ A proceeds.
So, if A □ B and B □ C, then B has jurisdiction over claim C □ A. The integral nexus between the plaintiff and defendant in a traditional jurisdictional analysis is that both have independent relationships to the state. Thus, A has a social responsibility to be part of an adjudication with respect to its actions toward C as a consequence of its relationship with B. This type of inquiry places the claim in the context of the broader universe
of social relationships of the defendant in the state, what might be termed a universalist approach.
144 Mesosystem level analysis focuses attention on interpersonal dynamics and the dynamics between the individual and secondary settings, such as work. BRONFENBRENNER, *supra* note 139, at 209.
145 The *Calder* analysis could be mapped as follows: A (the defendant) engages in conduct involving C (the plaintiff) whom A knows to be a resident of B (the state). So, under *Calder*, if A □ C and C □ B, then claim C □ A proceeds. Under *Calder*, the integral nexus between the plaintiff and defendant is the litigation, and only the plaintiff necessarily has an independent relationship with the state. As such, the social responsibility of the defendant to the state for its actions with respect to a resident is grounded only in the defendant's relationship to a particular resident and not the state as a whole. The *Calder* jurisdictional approach, as interpreted by subsequent decisions, is tautological: it turns entirely on the claim at issue and not systemic or individual level concerns. It examines the claim solely in the context of the relationship of the litigants, not the broader universe of social relationships of the defendant in the state, engaging in what might be termed jurisdictional relativism.

b. The need to provide incentives for entrepreneurship.—
Professor Geist argues, In an e-commerce context, the targeting test ultimately establishes a tradeoff that should benefit both companies and consumers. Companies benefit from the assurance that operating an e-commerce site will not necessarily result in jurisdictional claims from any jurisdiction worldwide. They can more confidently limit their legal risk exposure by targeting only those countries where they are compliant with local law.146 Two assumptions in the preceding quote are worthy of note. The preceding quote implicitly presumes that: (1) the "consumer" is not a corporate entity and that the content provider is and (2) the standard of "not necessarily result[ing]" in jurisdiction is adequate certainty for content providers to limit liability. First, as a practical matter, the targeting test has not been necessary in an e-commerce context. Single act jurisdiction in connection with purchases of physical products is firmly established147 and an e-commerce purchase and sale of a product would, in a vast majority of instances, satisfy a traditional minimum contacts analysis.148 The Internet has enabled entrepreneurs, particularly informational entrepreneurs such as online newspapers, who can not afford a storefront in physical space to set up virtual storefronts. An effects/targeting approach potentially disempowers such entrepreneurs in certain situations, for example, in litigation against a deep pocket corporate user. Unfortunately, a calculus sufficiently amorphous to provide only assurance that one will "not necessarily" be haled before the courts of a particular jurisdiction gives no comfort to a content producer for whom even one foreign suit would result in financial devastation. The effects/targeting approach simply does not provide clear guidance for contentproviders attempting to limit liability.

Further, Professor Geist points to the adoption of a targeting approach by the Securities and Exchange Commission (SEC) with regard to Internet

146 Geist, *supra* note 2, at 1404.
147 *See, e.g.*, Burger King Corp. v. Rudzewicz, 471 U.S. 462, 476 n.18 (1985).
148 At least two cases have analyzed an effects/targeting approach in connection with an eBay purchase. *See* Winfield Collection, Ltd. v. McCauley, 105 F. Supp. 2d 746, 749 (E.D. Mich. 2000); Metcalf v. Lawson, 802 A.2d 1221, 1226 (N.H. 2002). In both cases, the courts found that the seller could not control the jurisdiction of the purchaser. Therefore, the courts reasoned that it was not fair to subject the seller to jurisdiction in the forum of the purchaser. The courts' reasoning is in error. It is common that eBay sellers place specific jurisdictional restrictions on the areas from which purchasers may come. A seller retains the right on eBay to reject a purchaser's winning bid if the purchaser does not comport with restrictions that the seller set forth on the auction webpage. Thus, by completing the sale of the auctioned product, the seller accepted the purchaser's consideration on the terms the purchaser offered, which included the purchaser's residence in a particular jurisdiction. Sellers frequently specify jurisdictions into which they will not sell as terms of sale. In contrast, a website is never physically sent into a jurisdiction. It is only capable of being viewed in various jurisdictions. In order to permit a website to "be" in a particular jurisdiction, a user must download or cache the website. As such, this storage is a unilateral act of a third party; unilateral acts of third parties do not provide adequate basis for jurisdiction. *See, e.g.*, GTE New Media Servs., Inc. v. BellSouth Corp., 199 F.3d 1343 (D.C. Cir. 2000).

communications as an indication of its viability.[149] However, it might be argued that this approach is pulled out of its regulatory context and that viewing this targeting approach outside of the broader framework of securities regulations explicitly designed to protect entrepreneurship[150] is misplaced. Securities regulations on both the national[151] and state[152] levels set forth minimum thresholds of numbers and types of purchasers or prospective purchasers[153] to whom entrepreneurs can issue securities without triggering registration requirements.[154] Entrepreneurship and capital formation facilitation are central to the SEC's mission.[155]

c. The need for technology neutrality.—Although Professor Geist supports the quality of technology neutrality in a jurisdiction regime, his framework implicitly demonstrates an inherent preference for high technology[156] over low technology solutions to control for targeting. Specifi-

[149] Professor Geist correctly indicates that the SEC has adopted a similar "targeting" approach in its determinations. Geist, *supra* note 2, at 1383. However, this approach has been criticized and may be an inferior approach in the context of national securities regulation as well as jurisdiction determinations. For a more recent discussion of the SEC's approach to Internet registration, see Sec. & Exch. Comm'n, *Summary of Comments on Proposed Rule and Rule Amendment under the Investment Advisers Act of 1940 Addressing SEC-Registration of Internet Investment Advisers* (Sept. 25, 2002), *at* http://www.sec.gov/rules/extra/s71002commsumm.htm.

[150] The Securities and Exchange Commission has always viewed its mission as three-fold: capital formation, market stability, and consumer protection. *See, e.g.*, Stephen M. Cutler, Remarks at the University of Michigan Law School (Nov. 1, 2002), *available at* http://www.sec.gov/news/speech/spch604.htm. To pull the consumer protective targeting approach of the SEC outside the context of the other two goals of capital formation and market stability misses two-thirds of the SEC's calculus.

[151] On the national level, Regulation D, 17 C.F.R. §§ 230.504-06, explicitly exempts certain types of offers and sales of securities from the registration requirements of section 5 of the Securities Act of 1933, 15 U.S.C. §§ 77a *et seq*. (as amended).

[152] *See, e.g.*, Illinois Securities Law, 815 ILCS 5/4G (1999).

[153] Frequently, the ability to sell is restricted to "accredited investors," *see, e.g.*, 17 C.F.R. § 230.504, and to a small number of "unaccredited investors" under federal securities law. An "accredited investor" is defined in Rule 501 of Regulation D as:

(1) a bank, insurance company, registered investment company, business development company, or small business investment company; (2) an employee benefit plan, within the meaning of the Employee Retirement Income Security Act, if a bank, insurance company, or registered investment adviser makes the investment decisions, or if the plan has total assets in excess of $5 million; (3) a charitable organization, corporation, or partnership with assets exceeding $5 million; (4) a director, executive officer, or general partner of the company selling the securities; (5) a business in which all the equity owners are accredited investors; (6) a natural person who has individual net worth, or joint net worth with the person's spouse, that exceeds $1 million at the time of the purchase; (7) a natural person with income exceeding $200,000 in each of the two most recent years or joint income with a spouse exceeding $300,000 for those years and a reasonable expectation of the same income level in the current year; or (8) a trust with assets in excess of $5 million, not formed to acquire the securities offered, whose purchases a sophisticated person makes.

17 C.F.R. pts. 230, 239 (2003).

[154] In most instances, either a mere notice filing is required or, in many states, exemptions are selfexecuting and no notice is required. *See, e.g.*, Illinois Securities Law, 815 ILCS 5/4G(4).

[155] *See supra* note 150.

[156] This reliance on using the most current technology to connect users of networks to a particular geophysical location results in a technological arms race of sorts. Content providers will find them98:

cally, Professor Geist points to the efficacy of geolocation technologies.[157] Geolocation technologies, while demonstrating relatively high levels of accuracy for marketing purposes, are still imperfect, both for the Internet and other forms of Network Communications;[158] they do not offer adequate levels of certainty for jurisdiction purposes to be mandated as the tool of choice for jurisdictional determinations. For example, the European Union believes that geolocation technologies are inadequate tools for the purpose of assessing value-added tax on e-commerce.[159] A high-technology-based jurisdiction standard that imposes all costs of jurisdictional certainty on content providers is suboptimal. It increases the risk of compromise to sensitive user data and financially burdens small content providers, while infantilizing users. For many content providers, implementing geolocation filtering on their data flows will entail adding this additional step in the handling and storage of data, some of which will be personally identifiable financial data, through outsourcing data flows to third-party geolocation service providers[160] or performing the services inhouse.

Also, technological circumvention of geolocation by an increasing number of users is an inevitability. The potency of self-declaration, a low technology solution that relies on a particular graphical user interface construction, should not be minimized. Self-declaration may present a superior, patent vehicle for jurisdictional certainty than reliance on latent involuntary data gathering through methods such as geolocation.[161] A high-technology contingent jurisdiction regime is not necessarily as cost-efficient for either users or the court system. A corollary benefit also arises in a self-declaration based regime—the existence of contractual relationships inherent in every website is affirmed. By providing data regarding jurisdictional affiliation, a user provides consideration to the content provider for use of the website. As such, a stronger relationship is formed with regard to mu-

selves constantly upgrading technological capabilities to foil the ability of users to hide their physical location through technological circumvention of geolocation.

157 Geist, *supra* note 2, at 1401.

158 *See, e.g.*, Reuters, *911 Calls Not Easy To Pinpoint*, WIRED, June 22, 2003, *available at* http://www.wired.com/news/wireless/0,1382,59356,00.html.

159 ITAA, Ecommerce Taxation and the Limits of Geolocation Technologies, *available at* http://www.itaa.org/taxfinance/docs/geolocationpaper.pdf (last visited Jan. 7, 2004).

160 For a description of third-party geolocation service providers, see Caslon Analytics, *at* http://www.caslon.com.au/securityguide9.htm.

161 Specifically, Professor Geist points to the *iCraveTV* case as an indication of the impotence of self-declaration of users. *See* Twentieth Century Fox Film Corp. v. iCrave TV, No. 00-121, 2000 U.S. Dist. LEXIS 11670 (W.D. Pa. Feb. 8, 2000). This case can be interpreted otherwise and does not necessarily question the potency of self-declaration as a method of private ordering for jurisdictional certainty where the content provider has no additional basis for information. Of course, should a content provider wish to supplement self-declaratory information obtained from users with additional geographic information from, for example, geolocation technologies, a content provider may do so. However, aiming for a low technology, transparent approach presents an inclusive vehicle that acknowledges the agency of both users and content producers.

tual obligations, as articulated in the websites' terms of use and privacy policy, and the fiduciary relationship of the content provider.

5. Crafting a New Approach to Jurisdiction To Reflect the Shift in Economic Identity.—As seen in the discussion above, neither existing Internet-specific approaches, nor an approach grounded in the traditional jurisdiction doctrine of the "effects test" and the derivative targeting approach, contemplate the exchange of information going on through a website from the perspective of content provider data collection. Jurisdiction doctrine has been framed solely around a knee-jerk finding of jurisdiction in *Inset*. It has been structured around the website's user-perceived physical construction through the sliding scale approach (and not in terms of the website's actual activities) of *Zippo*. Finally, it has revolved around the relationship between the defendant's harmful conduct and the plaintiff, whom the defendant knows to reside in a particular forum through the effects test/targeting approach, instead of the relationship of the defendant and the forum. Consequently, jurisdictional determinations offer both inadequate predictability for business uses of the Internet and inadequate protection for individual users.

None of the current jurisdictional approaches to Internet activity (1) examine the actual construction and capabilities of the website *as known by the content provider*, including the extent of data gathering capability; (2) examine the relationship of the website to the forum in the absence of any injury; or (3) view the construction of jurisdictional certainty as a beneficial result for both content providers and users and, consequently, a result toward which both should cooperate. It is these three concerns that the Trusted Systems framework proposed in Part II seeks to address. In Part II, I argue that, because of the informational disparity of power in favor of content providers in Network Communications, a fiduciary relationship of sorts exists between a content provider and content users, which turns on the extent of the data being collected about users.[162]

Fundamentally, Part II presents a technologically neutral, transparent, and cooperative jurisdiction framework that relies on the three components that Professor Geist correctly identified—contract, technology, and express or implied knowledge of users—but places them into a new framework. This new framework is sensitive to network structure and is based on the constructs of consent and mutual social responsibility

[162] With increased releases of information, potential for its misuse or theft increased. From 1999 to 2002, the number of identity theft complaints filed with the Federal Trade Commission doubled every year. FED. TRADE COMM'N, OVERVIEW OF THE IDENTITY THEFT PROGRAM 1 (2003), *available at* http://www.ftc.gov/os/2003/09/timelinereport.pdf. Between 1998 and 2000, Internet penetration in the United States also almost doubled, going from approximately 26 percent to approximately 42 percent. NAT'L TELECOMM. & INFO. ADMIN., U.S. DEP'T OF COMMERCE, FALLING THROUGH THE NET: TOWARD DIGITAL INCLUSION (2000), *available at* http://www.ntia.doc.gov/ntiahome/fttn00/Falling.htm#2.

through voluntary self-declaration of both content providers and users. An approach that relies on user and content provider mutual self-disclosure presents a superior vehicle for jurisdiction purposes than one that imposes all costs on only one side of the content provider-user equation. Through mutual self-disclosure, content providers and users can create a de facto mutual consent to jurisdiction.

From this fiduciary relationship grounded in data collection spring two sets of obligations of fair information on content providers: fair disclosure obligations and fair conduct obligations. Fair disclosure obligations turn on contractual relationships between online entities and their users regarding, among other things, the extent and methods of data collection. Because data collection and use practices are not always patently obvious to users, a statutory obligation and business norm of disclosure through contract has been instituted. These contractual privacy promises, though rooted in a construct of private ordering, are enforced by mechanisms of coercion by the state.[163] Fair conduct obligations, on the other hand, pertain to the noncontractual obligation of the content provider not to intentionally harm users and other content providers. It is in connection with enforcing these fair conduct obligations in the court system that issues of jurisdiction more frequently arise. Indeed, a vast majority of Internet jurisdiction cases have arisen in connection with allegations of intentional torts and intellectual property harms. These are the "tough cases." Therefore, it is jurisdiction determinations in connection with precisely these two types of harms that the following jurisdictional approach hopes to address.[164]

II. SHIFTING CURRENT JURISDICTION FRAMEWORKS TOWARD THE MIDDLE AND RECOGNIZING THE IMPORTANCE OF INFORMATION MARKETS

As articulated in the preceding sections, inconsistencies exist in the application of current Internet jurisdictional approaches. Consequently, a prudent course of action may be to return to traditional jurisdictional standards, wielding a fresh perspective on the shortcomings of the Internet jurisdiction frameworks applied to date.

163 The Federal Trade Commission, among other agencies, actively enforces the privacy promises made in online privacy policies. *See, e.g.*, Consent Decree & Order for Civil Penalties, Injunctive & Other Relief, United States v. Hershey Foods Corp. (Feb. 2003), *available at* http://www.ftc.gov/os/2003/02/hersheyconsent.htm. Also, courts have enforced privacy promises in privacy policies made by websites, even in bankruptcy. *See, e.g.*, Fingerhut Bus. Servs., Inc. v. Etoys, Inc., No. 01-0064, 2001 WL 1640075, at *1, 7 (D. Minn. Sept. 6, 2001).

164 On a broader level, however, I would argue that a successful approach to fair conduct obligations is one that also incorporates fair disclosure obligations. In other words, a successful technologyneutral approach to jurisdiction is one that incorporates dialogue of content providers and users through Network Communications to set the terms of expected conduct.

A. Traditional Bases of Jurisdiction

Constitutional due process requires that a court only find jurisdiction when a nonresident defendant has adequate "minimum contacts"[165] with the forum in which the plaintiff has filed suit "such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice"[166] and "such that [the defendant] should reasonably anticipate being haled into court there."[167] To support a court's finding of general jurisdiction over a defendant, the court must find that the defendant "purposefully availed itself of the privileges of conducting activities within the forum State, thus invoking the benefits and protections of its laws" though "substantial" or "continuous and systematic" contacts.[168] For a court to establish specific jurisdiction over a defendant, it must find that a defendant's contacts were purposefully directed at the forum and that the litigation arose out of those contacts,[169] which "proximately result from actions by the defendant himself that create a substantial connection within the forum State."[170]

A three-part test determines whether the exercise of specific personal jurisdiction over a nonresident defendant is appropriate: (1) whether the defendant had sufficient "minimum contacts" with the forum state, (2) whether the claim asserted against the defendant arises out of those contacts, and (3) whether the exercise of jurisdiction is reasonable.[171] From a constitutional standpoint, the key inquiry of the minimum contacts analysis is embodied in the first question of "whether the defendant purposefully established" contacts with the forum state.[172] "[T]he foreseeability that is critical to the due process analysis is . . . that the defendant's conduct and connection with the forum State are such that he should reasonably expect to be haled into court there."[173] Defendants are, in this manner, protected from being forced to answer for their actions in a foreign jurisdiction based on "random, fortuitous or attenuated" contacts[174] and assured that an exer-

165 Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945) (citations omitted).
166 *Id*.
167 World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980) (citations omitted).
168 Hanson v. Denckla, 357 U.S. 235, 253 (1958) (citing *Int'l Shoe*, 326 U.S. at 319); *Int'l Shoe*, 326 U.S. at 317.
169 *Int'l Shoe*, 326 U.S. at 319–20.
170 *Id.* Five additional "fairness" factors are considered following a finding by a court of sufficient minimum contacts by the defendant in the forum: (1) whether a finding of jurisdiction would meaningfully inconvenience the defendant by forcing the defendant to defend in the forum; (2) whether the forum state has a meaningful interest in the adjudication of the dispute in the case; (3) whether the plaintiff has a meaningful interest in obtaining convenient and effective relief; (4) the court system's interest in efficiently resolving conflicts between diverse parties; and (5) the interests of states in judicially upholding certain social policies. Burger King Corp. v. Rudzewicz, 471 U.S. 462, 476–77 (1985) (citing *World-Wide Volkswagen*, 444 U.S. at 292).
171 *Burger King*, 471 U.S. at 474–75 (citations omitted).
172 *Id.* at 475 (citing *Int'l Shoe*, 326 U.S. at 319).
173 *World-Wide Volkswagen*, 444 U.S. at 297.
174 *Burger King*, 471 U.S. at 475 (citing Keeton v. Hustler Magazine, Inc., 465 U.S. 770, 774 (1984)).

cise of jurisdiction is "reasonable," without unfairly inconveniencing the defendant[175] and offending "traditional notions of fair play and substantial justice."[176]

B. A Trusted Systems Approach

As discussed above, Internet jurisdiction approaches adopted by courts in connection with claims involving allegations of intentional torts or harms relating to intellectual property in connection with Network Communications are inconsistent and frequently unpredictable. The sliding scale approach, although still in use, is fatally flawed and will continue to lose favor with many courts or be supplemented with other frameworks. The targeting approach will undoubtedly continue to be one such supplemental framework; it is gaining a following in case law.

However, at this juncture, it might prove useful to propose a different approach, which I call a "Trusted Systems" approach. The Trusted Systems approach attempts to accomplish four goals. First, it aims to be more sensitive to the way harms occur in connection with Network Communications than either the sliding scale or effects/targeting approach, while balancing the need for intellectual entrepreneurship. Second, it hopes to work with, instead of against, the structural realities of Network Communications, while preserving technology neutrality. Third, this approach strives to reflect the fundamental changes in economic identity and corporate citizenship described in Part I. Finally, this approach aspires to be a small step toward catalyzing greater discourse regarding jurisdictional harmonization of U.S. and E.U. standards in connection with intentional torts and intellectual property harms arising out of Network Communications.

The Trusted Systems approach is proposed here only in the context of jurisdictional determinations in connection with allegations of intentional torts or intellectual property harms arising out of Network Communications for two reasons. First, as a practical matter, these two categories of cases compose almost the entirety of the Internet jurisdiction case law, arguably turning it into a systemically critical inquiry. Second, by approaching this inquiry from a narrow scope, I attempt to circumscribe the negative effect of this approach on traditional jurisdiction doctrines. In this manner, I both acknowledge the unique nature of Network Communications and the jurisdictional problems they cause, while leaving untouched the vast majority of jurisdiction precedent.

1. The "Orientalized" Nature of Intentional Torts and Intellectual Property Harms.—Intentional torts and intellectual property harms that occur through Network Communications are inherently an "orientalized"[177]

175 *World-Wide Volkswagen*, 444 U.S. at 292.
176 *Int'l Shoe*, 326 U.S. at 316 (quoting Milliken v. Meyer, 311 U.S. 457, 463 (1940)).
177 The concept of orientalization is borrowed from Edward Said and, here, loosely refers to con

construct. By this term, I mean that certain harms exist because of and are defined in terms of an "other"—people outside of the plaintiff and defendant. For significant harm to arise out of the commission of certain intentional acts (or, in some instances, in order for their commission to occur at all) an engaged audience must be present, an "other," outside of the plaintiff and defendant that innocently participates in or witnesses the harm.[178] If an "other" cannot be constructed within a particular forum in which the defendant has a social responsibility for fair information practices, jurisdiction is not appropriate.

By way of example, I will apply this concept of "othering" to a case involving an allegation of Internet defamation[179] and a case involving an allegation of Internet trademark infringement.[180] In defamation, without an "other," an audience of a critical mass within a particular forum that is familiar with the plaintiff, it is unlikely that significant reputational damage will occur to the plaintiff within that particular geographic forum.[181] Therefore, logically speaking, in order for a Florida plaintiff to have been defamed in Florida by the online publication of an Alaska newspaper, an audience of a certain size in the particular part of Florida must have been aware of the allegedly defamatory statements and familiar with the plaintiff. If no such audience existed, it is unlikely that the plaintiff suffered significant reputational damage in Florida. Therefore, a finding of jurisdiction over an Alaska defendant in Florida is illogical in such a case. In fact, a finding of jurisdiction by a court in Florida is more likely to be playing into

struction of an identity by basing it on an "other." EDWARD W. SAID, ORIENTALISM 39–40 (1979).

178 The vast majority of Internet jurisdiction cases have arisen in the context of allegations of defamation, trademark infringement, and copyright infringement. *See, e.g.*, Rice & Gladstone, *supra* note 14, at 601. However, the framework would similarly pertain in cases involving allegations of misrepresentation and trespass. In misrepresentation, without a particular assertion being "held out" to the an audience of a critical mass, no misrepresentation necessarily knowingly occurs within that forum. In Internet trespass, the purpose of the trespass may be to obtain or divert information. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069 (N.D. Cal. 2000). Therefore, without an audience of a certain size in a state seeing that information as a consequence of and in context of the trespass, that state's interest in the trespass may not be significant. Of course, the plaintiff may always bring suit in the defendant's forum.

179 A prima facie cause of action for defamation usually involves the communication to a third person of allegedly false information that is understood to be defamatory by the defendant about the plaintiff. It must cause damage to the plaintiff. WILLIAM L. PROSSER, LAW OF TORTS § 111 (4th ed. 1971).

180 A plaintiff in a trademark case must demonstrate that the defendant's use of a mark has caused a likelihood of confusion regarding the origin of the defendant's goods or services. To demonstrate this, the plaintiff must show that it has developed a protectable trademark right in the trademark. The plaintiff then must demonstrate that the defendant is using a confusingly similar mark in such a way that it creates a likelihood of confusion, mistake, or deception with the public. To analyze whether a particular alleged infringement demonstrates a "likelihood of confusion," courts have generally looked at, among other factors, evidence of actual confusion by consumers. *See, e.g.*, Taubman Co. v. Webfeats, 319 F.3d 770, 776–77 (6th Cir. 2003).

181 For a discussion of the culturally specific construction of the nature of defamation regarding the extent of the required audience, see Daniel More, *Informers Defamation and Public Policy*, 19 GA. J. INT'L & COMP. L. 503 (1989).

a plaintiff's tactic aimed at causing meaningful procedural inconvenience to the defendant rather than furthering a plaintiff's legitimate quest for remediation of actual damages.

Similarly, in the context of trademark infringement, without an "other," a critical mass of individuals in a particular forum who see content that infringes a third party's intellectual property, that state's need to protect its citizens from a likelihood of confusion is not sufficient to warrant that state's exercise of jurisdiction over a particular defendant. There are other forums available with a more direct interest in the alleged infringement, such as the defendant's state. If, however, a plaintiff demonstrates that a critical mass of citizens within the jurisdiction have been potentially confused as a consequence of the alleged infringement, the state would be reasonable in exercising jurisdiction over the defendant.[182]

From this construction of intentional torts and intellectual property harms arising out of Network Communications in terms of an "other," it can be argued that the presence or absence of this "other" and the size of this constituency articulates to what extent a state, as the political embodiment of the collectivity of citizens, has an interest in an alleged harm. Thus, I would argue that the size of the "other" should play a role in jurisdictional determinations in connection with intentional torts and intellectual property harms arising out of Network Communications. This assertion is intellectually rooted in insights regarding the structure and stability of networks and the relative impacts of different actors within the network.

2. Power Laws, Nodes, Hubs and Network Theory.—Network theory, a school of thought revolving around the dynamics of interactions of various actors within and across groups, postulates that two types of network structures exist—scaled and scale-free.[183] Scaled networks present networks in which every point in the network has approximately the same relationship to most other points in the network, such as the network of highways in the United States.[184] Scale-free networks, on the other hand, consist of different points or "nodes" in the network; the different nodes

[182] Many of the early Internet-related disputes were based in intellectual property issues that, were they to be litigated today, likely would be resolved through other means, such as the International Corporation of Assigned Names and Numbers Uniform Dispute Resolution Procedure, *at* http://www.icann.org/udrp/udrp.htm. In particular, in proving a case in the ICANN UDRP proceedings, plaintiffs rely on the elements of cybersquatting set forth in the Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d) (2000), which was passed in 1998—a year after *Zippo* was decided. Thus, it can be argued that reliance on domain name dispute precedents prior to the ACPA and their extension into e-commerce and m-commerce (commerce taking place through "wireless handheld devices, such as cellular phones and personal digital assistants," Whatis.com, Definition: m-commerce, *at* http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci214590,00.html (last visited Oct. 29, 2003)) cases is misplaced, particularly when the legal and regulatory climate in which the dispute arose has fundamentally changed.

[183] BARABASI, *supra* note 28, at 55–72.

[184] *Id.*

evidence drastically different levels of connectivity—some nodes are connected to a very large number of other nodes, and some nodes are connected to only a few others.[185] As a consequence, one cannot predict the number of connections a particular node has because no average can be calculated.[186]

The distributions of these nodes and the extent of their connectivity does not fall along a bell curve but, rather, follows a "power law."[187] Power laws are articulations of patterns that are not random, but have no typical node.[188] In random networks, at the peak of the distribution, one assumes that a majority of nodes reflect the same number of links; nodes that have a significant difference in the number of links are an aberration.[189] But, in a power law-driven distribution, no typical node exists and the network is composed of a continuous hierarchy of nodes with a few "hubs"[190] and numerous small nodes.[191]

The proper classification of the Web is as a scale-free network, which is characterized by the same patterns found in other scale-free networks in nature. As such, the Web is not a new or different governance space.[192] It is, however, a governance space that has usually been left to the forces of science rather than the forces of law.[193] As the Web expands, the question becomes not whether someone has the ability to post views or create an ecommerce website, but, rather, if users can find the created website to view it.[194] Similarly, an industry surrounding Internet[195] purchase intermediation has arisen in the form of online payment providers, and credit cards are used for the majority of Internet purchases.[196] Therefore, the issue facing entrepreneurs is increasingly not the technological obstacle of content creation, but rather ensuring that their created content is found by users[197] and that any liability arising out of the content and users' actions on the website, including any transactions, is limited. The sign of a website's potency and accessibility is, perhaps most importantly, how many other websites hyper-

185 *Id.*
186 These observations of power laws date back to Pareto. *Id.*
187 *Id.*
188 *Id.*
189 *Id.*
190 Hubs are nodes with a disproportionately large number of nodes connected to them. *Id.* For example, Google (www.google.com) is, as of this writing, a hub.
191 Erdos and Renyi's random network theory, as extended by Watts and Strogatz, asserted that the number of nodes with a particular number of links decreases on an exponential basis, which is a rate of decay that is swifter than the rate predicted by a power law. *Id.* at 56.
192 *Id.* at 55–72.
193 *Id.*
194 *Id.*
195 When used in this Article, Internet refers to Network Communications outside the Web (such as email), as well as those on the Web, unlike the interchangeable usage used by many courts and other authors.
196 *Id.* at 55–72.
197 *Id.* at 57.

link to it.[198] These links are not random in their nature, however.[199] Some websites are heavily linked to and constitute hubs within the network.[200] Thus, this organizational structure of the Web (and presumably the organizational structures of future Network Communications) will inherently impact the operationalization of any legal overlay.

3. Purposeful Availment of Audiences and Data, Social Responsibility, and Consent to Jurisdiction.—Perhaps current jurisdictional frameworks in connection with intentional torts and intellectual property-related harms on the Web are in disarray because of our lack of sensitivity to Web network structure. Our current jurisdictional paradigms are premised on an intellectual construction of the Internet as a scaled network, where every actor is an equal node, just as every website appears equivalent. However, this intellectual construction is flawed. Not all websites, despite appearances to the contrary, are equal in the extent of their interconnectivity with other websites—some websites are mere nodes. As such, regulating hubs and nodes in an equivalent manner may not be logical. Therefore, I argue that a paradigm shift is required in our jurisdictional thinking from a scaled network approach to a scale-free network approach. In other words, the extent of a website's connectivity and the size of its audience matters.

Specifically, jurisdictional determinations in the context of cases involving allegations of intentional torts or intellectual property harms arising out of Network Communications should be intellectually reframed in terms of purposeful availment of an "audience" and the information market of a jurisdiction. When a content provider chooses to give access to its content to a critical mass of citizens within a particular forum,[201] the content provider chooses to purposefully avail itself of the forum; the content provider has received access to a significant audience (and that audience's data) for its commercial or noncommercial speech and has had opportunity to collect significant information[202] about both this audience of citizens and the information market of the particular forum. By engaging in content provision in exchange for[203] collecting (or having the opportunity to collect) geographi-

198 *Id.* at 55–72.
199 *Id.*
200 *Id.*
201 Specifically, this contemplates citizens whom the content provider knew or should have known were citizens of that forum.
202 Having the opportunity to collect significant information is demonstrated by the extent of technological data-gathering capabilities of the content provider.
203 This construction of the user-content provider relationship, which views user data as the consideration for providing content or services, is typical. Terms and Conditions of Use of websites are frequently authored on the basis of this exchange, setting forth user data as the consideration for supporting the agreement. *See, e.g.*, Yahoo!, Inc., Terms of Service, *at* http://docs.yahoo.com/info/terms/ (last visited Oct. 29, 2003).
In consideration of your use of the Service, you represent that you are of legal age to form a binding contract and are not a person barred from receiving services under the laws of the United

cal information and other data with a number of unique users in excess of a certain bright-line minimum threshold number, a content provider knowingly enters the information market of that jurisdiction and purposefully avails itself of the benefits of the forum. This purposeful availment, in turn, results in social responsibility to the audience within that jurisdiction. By entering the information market of a jurisdiction, a content provider accepts a higher level of social obligation for maintaining the stability of that jurisdiction's and our society's "trusted systems" of economic and information exchange. As a consequence of this fiduciary position within the trusted system of a jurisdiction's information market, the content provider consents to jurisdiction within the forum in connection with allegations of intentional torts and intellectual property harms. However, until a content provider reaches the minimum threshold number of unique users within a particular jurisdiction, the content provider has not purposefully availed itself of user data within that forum and is not subject to the jurisdiction of courts within that forum in connection with allegations of intentional torts or intellectual property harms; there is no "other" in the jurisdiction around whom harms allegedly committed by the defendant can be constructed. The content provider, of course, remains subject to the jurisdiction of courts in states with a preexisting jurisdictional interest in the content provider (e.g., the content provider's state of incorporation or principle place of residence). Therefore, at issue is not whether the content provider can be brought in front of a court for the allegedly bad acts, but solely where the claim is best brought.

In order to establish that a content provider has purposefully availed itself of the benefits of (access to the data or citizens of) a jurisdiction in connection with a jurisdictional inquiry arising from an allegation of an intentional tort or intellectual property-related harm through Network Communications, a plaintiff must demonstrate that a certain number of citizens known by the defendant to be accessing the website from the jurisdiction were provided access by the defendant to its network content,[204] thereby causing the defendant to have a social responsibility to the particular forum.

Thus, the appropriate jurisdictional question to ask, in the context of an alleged intentional tort or intellectual property harm arising out of the Web and, perhaps other Network Communications, is whether the defendant has con-

States or other applicable jurisdiction. You also agree to: (a) provide true, accurate, current and complete information about yourself as prompted by the Service's registration form (such information being the "Registration Data") and (b) maintain and promptly update the Registration Data to keep it true, accurate, current and complete.
Id.

204 As a practical matter, this type of discovery would not be expected to be burdensome. Most websites keep extensive databases regarding the profiles of their users. Many websites require registration for access and such registrations frequently require a zipcode or state of residence to be provided. *See, e.g.*, The New York Times Co., Online Registration, *at* http://www.nytimes.com/auth/login?URI=http://www.nytimes.com/packages/html/business/2003davis_double.html.

sented to the jurisdiction of the forum's courts and accepted social responsibility to a critical mass of citizens.

By constructing a jurisdictional regime around mutual self-declaration of both the content provider and the user, a relationship is fostered between both the users and providers, as well as providers and forums. Just as in First Amendment contexts, mandated counterspeech presents a preferable remedy to a prohibition on speaking. The operationalization of this self-declaration could come through numerous presentations, including a clickwrap agreement, an interactive map, state specific counters, or an online depository of user recourse information.[205] In this manner, website users will also obtain additional external indicators and representations of recourse available to them. Responsible websites will act transparently, disclosing the jurisdictions where they do business. In this manner, they would demonstrate their interest in protecting their users and generating good public relations. Increased levels of trust between content-providers and users are a likely outcome.

4. The Trusted Systems Approach and Jurisdiction Paradigms—Consensual Social Responsibility.—In cases involving allegations of intentional Internet torts and intellectual property harms on the Web, courts should look to the dynamic structure of the network in lieu of a targeting approach. The Web and subsequent generations of Network Communications should be viewed as scale-free networks in which several "hubs" have a disproportionate impact on the stability and activity on the network. Conversely, the majority of other websites are mere "nodes" whose activities do not have a significant impact on the perceived or real stability of the network. As such, at the point a node chooses to become a hub within a particular jurisdiction by providing content to a certain number of unique users, it enters into a type of contractual arrangement with the forum whereby it accepts a higher level of social responsibility for the stability of the network within the forum.

It is logical for claims from various jurisdictions where the website is a node to be centralized in jurisdictions where the website has chosen to become a hub and thus has accepted a higher level of social responsibility to

[205] For example, one way to operationalize the graphical user interface construction of the disclosure I am proposing would be a clickwrap dialogue box pop up asking the user's state and country of residence. It would offer simultaneously, and as theoretical consideration for this information, a global interactive map similar to the map of the United States available from the Federal Trade Commission in connection with their Consumer Sentinel project at http://www.consumer.gov/sentinel/. On this "recourse map," users would be able to see the jurisdictions in which the content provider has many known users and is subject to jurisdiction. This interface construction will serve to build trust by providing users with a clear indication of the extent of business an entity conducts within their geographic area and whether their opportunity for recovery would be limited by jurisdictional concerns. When the user provides her state of residence, her state is added to the running tally of users of the website in that state. At the point that the number of users exceeds the "magic number" of users adequate to trigger jurisdiction, the interactive map would reflect this by changing the color of the state in question.

citizens of the forum. In this way, the hub jurisdictions, which have the greatest interest in the defendant's activities because more of their citizens are implicated, have more complete notice of claims arising out of the defendant's actions. Jurisdictions where the website is a hub may be more likely to levy substantial penalties if the content provider turns out to be a repeat offender. Simultaneously, small content providers receiving only a small amount of traffic from numerous jurisdictions are prevented from facing suit in each jurisdiction. In this way, the social value of informational entrepreneurship and the prevention of meaningful procedural inconvenience for defendants would be recognized.

Current jurisdictional approaches adopt a scaled network approach that treats all actors identically. Consequently, they provide an incongruous framework for regulation of intentional tort claims involving a scale-free network like the Web and, presumably, subsequent communication networks. Because the proposed approach involves a bright-line standard, its adoption would provide greater jurisdictional certainty to all actors in economic exchanges and would facilitate procedural due process. The proposed approach may also present a vehicle for successfully reconciling the stark contradictions inherent in existing Internet jurisdiction case law and pulling it into the body of jurisdiction case law as a whole. Finally, the proposed Trusted Systems approach is technologically neutral in character, which would lend it greater doctrinal longevity, and may articulate a position easier to harmonize internationally than current U.S. jurisdiction standards.[206]

Although I am advocating an approach in Part II premised partially on a construct involving private ordering through self-declaration, private ordering in general cannot be viewed as a panacea. Professor Perritt argues that private ordering provides legal certainty in an environment of jurisdictional confusion. In practice, an enforceable contract with clear terms is rarely in place in disputes arising out of Network Communications and, even if in existence, such agreements are not always enforceable. Perritt, however, acknowledges the critical role that courts play in actualizing parties' will in contract. As such, he recognizes the inherent limits in an exclusively privately-ordered solution.[207] Another form of private ordering

[206] Although I disagree with Stein in his denial that a new approach to jurisdiction is warranted, I agree with him that jurisdiction cannot be separated from the question of extraterritorial effects. Stein, *Frontiers of Jurisdiction*, *supra* note 2. As such, the inquiry of how to best address cases like *Yahoo! v. La Ligue Contre Le Racisme et L'Antisemetisme*, 169 F. Supp. 2d. 1181 (N.D. Cal. 2001), is complex. For one discussion of the *Yahoo!* Case, see Mark Rosen, *Exporting the Constitution: A Misconception Concerning the Enforceability of "Un-American" Judgments*, 53 EMORY L.J. (forthcoming 2004) (arguing the U.S. court wrongly refused to enforce the judgment of the French court). *But see* Molly S. Van Houweling, *Enforcement of Foreign Judgments, the First Amendment, and Internet Speech: Notes for the Next* Yahoo! v. LICRA (unpublished manuscript) (discussed in Rosen, *supra*) (arguing that the U.S. court correctly refused to enforce the judgment of the French court).

[207] Perritt, *supra* note 2, at 249–51.

discussed by Allan Stein is third party-mediated private ordering through certification. Stein argues that jurisdiction determinations turn on normative judgments of substantive laws[208] and, citing Lessig,[209] that the use of digital certificates[210] will permit Internet actors to have knowledge of the identity of the party with whom they are communicating.[211] Thus, Stein appears to rely on the success of one particular technology that has failed to gain widespread acceptance.[212] Specifically, digital certificates have met with significant resistance in light of, among other things, certain technological inadequacies of public key infrastructure,[213] required digital certificates,[214] the extent of privacy invasiveness required by a full scale public key infrastructure,[215] the unreliability of certificate providers,[216] the inability of clients to understand the process and feel secure being part of it,[217] and the lack of widespread acceptance.[218]

However, construing Stein's point in perhaps a broader light than he intended, his argument can be interpreted to advocate using technological means to identify users in interactions on the Web and, thus, enable actors to limit jurisdictional exposure. Although Stein's position is becoming closer to reality in light of increased technological identification capabilities such as geolocation providers, the approach does not fully succeed. While many of these services boast success rates in the high 90 percent range,[219] these services cannot necessarily pinpoint a state where a user sits. Stein's reliance on technology to provide full disclosure of the jurisdictions touched by a website falls victim to the same problems of Geist's approach with regard to lacking technology neutrality. Both approaches are not fully sensitive to the way interactions on the Web occur at the present time, including the role of geolocation avoidance mechanisms, such as proxy serv-

208 Stein, *Frontiers of Jurisdiction*, *supra* note 2, at 394.
209 LESSIG, *supra* note 30, at 35, 38–39.
210 A digital certificate is an electronic credential that identifies a user or content provider on the World Wide Web and is issued by a certification authority. Ectag, Public Key Infrastructure (PKI), *at* http://www.ectag.org/ec/lawsecure/pki.htm (last visited Jan. 7, 2004).
211 Stein, *Frontiers of Jurisdiction*, s*upra* note 2, at 393 (citing LESSIG, *supra* note 30, at 38–39, 49–53).
212 "This technology thus offers a mechanism for a state to regulate extraterritorial behavior that has a state-specific impact without burdening extraterritorial behavior that does not have such impact." *Id.*
213 Roger Clarke, The Fundamental Inadequacies of Conventional Public Key Infrastructure, *at* http://civics.com/pki/InadequaciesOfPKI.htm (last modified May 3, 2001).
214 *Id*.
215 *Id.*; Andy McCue, *Digital Certificates Fail Government Project*, VNU.NET NEWS, June 20, 2002, *at* http://civics.com/pki/eEnvoySansCerts.htm.
216 McCue, *supra* note 215.
217 *Digital Certificates: A Solution in Search of a Problem*, FUTURE BANKER, Mar. 8, 2001, *at* http://civics.com/pki/SolutionWithoutProblem.htm.
218 *Id.*
219 See *supra* note 160 for discussion of geolocation providers.

ers,[220] and the limits of current network infrastructure.[221] Every website is not currently capable of identifying every user's jurisdiction without the cooperation of users. For these reasons, a self-declaration regime is a superior jurisdictional starting point.

It is true that some users will always refuse to cooperate with a selfdisclosure regime and purposefully obfuscate their jurisdictions. Such obfuscation can be construed as a user's waiver of interest in preserving the right to recourse in her jurisdiction in connection with intentional torts or intellectual property harms occurring on the website. To wit, by refusing to identify herself as a citizen of a particular jurisdiction, she did not express a preference for the courts of her jurisdiction. Meanwhile, a content provider should simultaneously inform users of the jurisdictions in which it consents to suit. Through such mutual information disclosure, trust is built between content providers and users, and jurisdictional certainty is more likely. Similarly, if users choose to deceive the content provider about their jurisdiction, and if the content provider does not have reason to otherwise know the users' jurisdictions (e.g., through a registration at some point in the website or voluntary use of geolocation), the content provider cannot reasonably be said to knowingly form a relationship with the deceptive users' real forum and be subject to its jurisdiction.[222]

This proposed framework, in a way, turns on its head Professor Brilmayer's argument regarding jurisdiction assertions and citizen participation in the democratic process. Professor Brilmayer argues that "[t]he basic inquiry must be whether the defendant's level of activity rises to the level of

[220] A proxy server is a server that acts as an intermediary between a browser and a real server with desired content, sometimes used to mask the identity of the user while relaying the request for content. Webopedia, *at* http://www.webopedia.com/TERM/p/proxy_server.html (last visited Jan. 7, 2004).
[221] *See* Clarke, *supra* note 213.
[222] Extrapolating this approach to an international and possibly criminal context may mean that, for example, a foreign citizen determined to read a U.S. website containing content prohibited in her country can misrepresent her country of residence to the content provider and, thus, possibly put the U.S. content provider in violation of her government's prohibition on supplying such content. Should a foreign government choose to prosecute such a content provider who had no user-declared information indicating the user's residence, the United States should vigorously defend the content provider as a matter of public policy. In a scenario such as this, the content provider engaged in a reasonable effort to ascertain the jurisdiction of user origin in order to limit liability and, potentially, show respect for a foreign government's law. Users' misrepresentations are neither the fault nor the problem of the content provider if the content provider chooses to use no other independent means of verification of user residence. Also, even if, for example, geolocation is used, the source of the data flow will not necessarily be geolocated to the appropriate country in light of technological avoidance mechanisms, such as taking several hops through anonymizing proxies. *See* Nick Feamster et al., Thwarting Web Censorship with Untrusted Messenger Discovery 1–2 (Mar. 2003), http://wind.lcs.mit.edu/papers/disc-pet2003.pdf. For a defense of the democratic importance of identity self-construction under oppressive political regimes and the Internet, see Andrea M. Matwyshyn, *Review of Prometheus Wired: The Hope for Democracy in the Age of Network Technology*, RESOURCE CENTER FOR CYBERCULTURE STUDIES, http://www.com.washington.edu/rccs/bookinfo.asp?ReviewID=191&BookID=166 (last updated Apr. 29, 2003).

activity of an insider, so that relegating the defendant to the political process is fair."[223] Instead, a Trusted Systems approach might give citizens a democratic voice in corporate governance and disposition of their data. In general, the two schools of jurisdictional thought revolve around, on the one hand, concepts of presence-based authority of the State to retain the right to control and adjudicate matters over anyone in its territory (the "contractarian" approach) and, on the other hand, effects-based authority in which the State retains the authority to provide restitution to its citizens for the damaging effects of actions that occur within the State (the "regulatory" approach).[224] The polarities of contractarian versus regulatory conceptions of jurisdiction, at least in the context of e-commerce, seem somewhat draconian.

In both cases, they bespeak of an overly centralized conception of governance and control. Perhaps the reason for the existence of the current jurisdictional morass in connection with certain harms occurring on the Web is that neither of these two jurisdictional paradigms fits with the more entrepreneurial, more economically egalitarian spirit pervading Network Communications. Perhaps it is not our traditional constructions of jurisdiction doctrine that need retooling, but rather the way we conceptualize the relationship between those over whom jurisdiction is asserted and the State. Both contractarian and regulatory approaches understate the agency of the plaintiff and defendant in connection with their relationship with each other and the agency involved in the defendant's relationship with the forum.

Jurisdiction is usually conceptualized as something that happens to defendants at the behest of courts, rather than something that arises out of a defendant's choice to take on a fiduciary relationship to citizens of a forum. Due to the low transaction costs of Internet entrepreneurship (e.g., costs associated with registering URLs, operating and creating content on websites, and purchasing "spammer" lists for facilitating advertising of product), small online ventures have burgeoned in the last five years.[225] Perhaps this rise of Internet entrepreneurship is forcing the development of a jurisdictional theory middle ground—a social contractarian approach to jurisdiction. This social contract is similar to the rationale articulated in traditional presence-based jurisdiction principles, as extrapolated in today's minimum contacts analysis, but it gives preemptive voice and agency to potential defendants. It revolves around potential defendants choosing to have access to audiences, in exchange for which they choose to assume the social responsibility of restitution for effects they cause within the forum. In other words, in exchange for submitting to jurisdiction within a particular state, a Web content provider purchases access to an audience over a certain size

223 Lea Brilmayer et al., *A General Look at General Jurisdiction*, 66 TEX. L. REV. 721 (1988).
224 For purposes of this theoretical discussion, the distinctions between general and specific jurisdiction, if there is a reason to have them, are ignored.
225 Indeed, every time I receive yet another herbal Viagra or penile enlargement email, I stop to marvel at the extent of this successful burgeoning.

within that state. The content provider is "given voice" for commercial or noncommercial speech to a particular known audience (about whom the speaker has particular information) in exchange for consenting to a social responsibility to the audience through becoming subject to jurisdiction.

This social contractarian approach is already used in the context of state securities regulation. When an entrepreneur is seeking to conduct a limited securities offering, in order to comply with blue sky laws,[226] the entrepreneur is frequently required to file a consent to jurisdiction if the securities are going to be offered or sold to more than a certain "magic number" of purchasers within the state.[227] However, until the entrepreneur makes offers or sales to prospective purchasers within that state over that magic number, a state usually does not deem itself to have a sufficient interest in being able to assert jurisdiction over the entrepreneur to warrant a consent to jurisdiction. In this way, states balance the need for capital formation, investment, and entrepreneurship with the need for citizen protection. This securities framework recognizes that consumers reach out to entrepreneurs as often as the inverse, and it allows for a level of jurisdictional certainty for the entrepreneur. Through a reliance on mutual self-disclosure, both entrepreneurs and prospective securities purchasers benefit. They become partners in business. If an entrepreneur wishes to avoid being subject to a particular state's jurisdiction, the entrepreneur will choose to forego selling securities to purchasers in this state in excess of the statutorily articulated threshold. This filtering of prospective purchasers is achieved, among other ways, through an investment questionnaire usually given to a prospective purchaser prior to the offering materials, which the issuer may choose to independently verify. In other words, the burden of ascertaining the jurisdiction in which the prospective purchaser resides is shared between the issuer and the prospective purchaser.

It is this type of cooperative framework of disclosure based partially in private ordering, which I argue is better suited for acquiring jurisdictional certainty in connection with claims involving intentional torts or intellectual property-related harms. Through mutual self-disclosure, content providers and content users become partners in Network Communications. Content providers will be able to control exposure to liability by making a conscious decision to enter or refrain from entering a particular jurisdiction, while users will simultaneously receive information from the content provider re-

226 State securities statutes are generally and popularly referred to as "blue sky laws" because they are meant to prevent "speculative schemes which have no more basis than so many feet of 'blue sky.'" Hall v. Geiger-Jones Co., 242 U.S. 539, 550 (1917).

227 The number depends upon, among other things, whether the prospective purchasers are "sophisticated" or "unsophisticated" investors (as such terms are defined within each state's blue sky law) and varies from state to state. *See, e.g.*, Illinois Securities Law, 815 ILCS 5/1-5/19 (1999). These definitions frequently mirror the definition of an "accredited investor" in the federal securities regulatory framework. *See supra* note 153 for the definition of an accredited investor under the Securities Act of 1933.

garding the availability of recourse in particular jurisdictions. Thus, both content providers and users are put into a better position to choose whether to form a relationship with each other.

C. Benefits of a Trusted Systems Approach

The benefits of a Trusted Systems approach to jurisdiction in connection with claims alleging intentional torts and intellectual property harms arising out of Network Communications are similar to those of a trusted computing base. A trusted computing base is a core set of protection mechanisms within a computer system intended to act as a fully secure foundation for operation of additional components of a system.[228] Although the remainder of the system may not be fully secure, the existence of the trusted computing base enables additional components to be layered on without concern regarding the ultimate integrity of the system.[229] For similar reasons, establishing a clear, predictable jurisdiction regime in connection with Network Communications is critical. A successful jurisdiction approach ensures access of the correct citizens to the appropriate courts in order to grant recourse for harms. A trusted jurisdiction basis ensures that this recourse for harms is always available on clear, predictable terms. Simultaneously, the presence of such a secure foundation facilitates societal experimentation with regulatory approaches in other areas of law. Therefore, even if subsequent regulatory or private ordering approaches to Network Communications (in areas outside of jurisdiction) fail, the presence of a trusted jurisdiction base guarantees overall systemic stability.
The elements of a trusted computing base include regulating access and authentication of users, granting authorization for using specific resources, and protecting against system infiltration.[230] These same elements describe the structure and functionality of a successful Network Communications jurisdiction paradigm.

1. Regulating Access and Authentication of Users and Authorizing Use of Particular Resources.—One of the premises of any jurisdiction regime is that not every claim should be heard in every court. Access to the court system of a particular jurisdiction is a scarce resource that is only meted out to appropriate individuals, those with a sufficiently strong connection with the forum. Conversely, our society similarly recognizes a due process concern in preventing defendants from being sued anywhere, particularly in forums to which they only have a tenuous connection. Thus, an efficient jurisdiction regime is one in which access to the court system's scarce resources is successfully regulated: access is only granted to appro-

228 Institute for Telecommunications Sciences, *at* http://www.its.bldrdoc.gov/fs-1037/dir-038/_5629.htm (last visited Jan. 7, 2004).
229 *Id.*
230 *Id.*

priate "users" of the court system in a manner that offers a high level of certainty for both plaintiffs and defendants.

The Trusted Systems approach to jurisdiction introduced in this Article provides a paradigm that regulates access of users to scarce resources in a manner that facilitates entrepreneurship in content production. Unlike Internet jurisdiction paradigms currently in use, the Trusted Systems approach enables both plaintiffs and defendants to predict the outcomes of jurisdiction determinations to a significantly greater degree. By requiring self-disclosure of users' jurisdictions and jurisdictions where the content provider has already "consented"[231] to jurisdiction, users and content providers are authenticated as individuals entitled to the benefits of the recourse structure of a limited number of known jurisdictions. Because of operationalization through a bright-line rule that includes a cushion of users in each jurisdiction prior to a content provider becoming subject to the courts of that jurisdiction, the mere fact of operating a website does not instantly subject a content producer to an unspecified number of jurisdictions. As a consequence, content entrepreneurship is stimulated because the liability risks associated with content entrepreneurship become lower. Entrepreneurs have notice when they are about to become subject to a particular jurisdiction's court system. Additionally, the hub-based structure of the Trusted Systems approach mirrors that of several other regulatory regimes in which we, as a society, are forced to balance innovation against redress for harm. For example, both the Workers Adjustment Retraining and Notification Act[232] and the Family Medical Leave Act,[233] like the Trusted Systems approach to jurisdiction, create a bright-line baseline number of individuals who must be impacted in a particular place before legal consequences follow for an entrepreneur.

Additionally, the Trusted Systems framework comports with due process concerns about avoiding meaningful procedural inconvenience for defendants; [234] because the jurisdiction inquiry turns on whether a theoretical consent to jurisdiction has occurred through amassing a critical number of contacts within a particular jurisdiction, an unintentional, tenuous connection to one user in a far-away forum would not suffice for jurisdiction in in-

231 After a certain number of user authentications from a particular jurisdiction, a content provider has consented to jurisdiction in the forum.

232 29 U.S.C. §§ 2101-09 (2000). The WARN Act requires that employers who employ over 100 workers and intend to close a plant in which at least fifty workers will lose their jobs provide at least sixty days notice to workers of the impending plant closure. In this way, the WARN Act balances the needs of employees to be able to plan the future of their employment with the need to exempt entrepreneurs from what may be perceived to be onerous notice requirements that would impair the conduct of the business.

233 29 U.S.C. §§ 2601-54 (2000). Under the Family Medical Leave Act, only employers who employ more than fifty employees are required to comply by providing a medical leave of absence at the employee's request.

234 *See generally* Redish, *supra* note 2.

tentional tort and intellectual property claims. Currently, a large percentage of content providers are already identifying the country or state of origin of a significant amount of Internet traffic for marketing purposes. Therefore, from a practical standpoint, few additional data collection burdens would be required under a Trusted Systems approach to enable content providers to limit their exposure in various jurisdictions. Through a jurisdictional approach centered on data collection, content providers receive both the benefit of being able to identify their user base more accurately and avoid being haled into courts of distant jurisdictions, while simultaneously being held accountable for the collection and use of an audience in the particular jurisdictions where they benefit from a significant audience for their commercial and noncommercial speech. In this manner, constitutional due process protections are incorporated to preserve systemic integrity.

2. Protecting Against System Infiltration.—With regard to protection against system infiltration, the Trusted Systems approach offers an easier starting point for multilateral cooperation and harmonization in constructing a global recourse structure to ferret out bad actors on an international basis. The bright-line test of the Trusted Systems approach provides greater certainty for both users and content providers. As such, this approach more closely resembles the bright line approaches frequently advocated by the European Union.[235]

Although the proposition of creating a bright-line operationalization of a minimum contacts analysis based on defendant's actual knowledge may be a controversial suggestion at first blush, it is not out-of-step with the intellectual deep structure of jurisdiction theory to date. As previously discussed, in general, the two schools of jurisdictional thought revolve around, on the one hand, concepts of presence-based authority of the State to retain the right to control and adjudicate matters over anyone in its territory (the "contractarian" approach) and, on the other hand, effects-based authority with the State retaining the authority to provide restitution to its citizens for the damaging effects of actions that occur within the State (the "regulatory" approach). The Trusted Systems framework incorporates both rationales and addresses the concerns expressed by the European Union in the course of negotiations of the Hague Convention on International Jurisdiction and Judgments in Civil and Commercial Matters (the "Hague Convention").[236] In the process of negotiating the Hague Convention, two of the primary incompatibilities between U.S. and E.U. jurisdiction principles, as articulated by the European Union, are the lack of predictability in a standard

235 *See, e.g.*, Linda Silberman, *Comparative Jurisdiction in the International Context: Will the Proposed Hague Judgments Convention be Stalled?*, 52 DEPAUL L. REV. 319, 325 (2002) (discussing current non-derogation from consumer's place of residence).
236 Hague Conference on Private International Law, *at* http://www.hcch.net/e/workprog/jdgm.html (last visited Jan. 7, 2004).

U.S. minimum contacts analysis and an overlitigious U.S. legal culture.[237] Jurisdiction in the European Union is determined for the most part by a series of bright-line rules.[238] In particular, in cases alleging intentional torts, such as defamation, jurisdiction is usually appropriate in the forum where the harm occurred, presumably the forum of the plaintiff's residence.[239] Meanwhile, in the United States, a jurisdiction calculus is composed of more qualitative, flexible components that do not present adequate certainty of recourse and protection from defending frivolous litigation for E.U. citizens.

When this perceived uncertainty is coupled with the E.U.'s general perception that the United States fosters a highly litigious legal culture, a theoretical impasse arises in creating a workable international jurisdiction framework, particularly in the context of Network Communications. However, an interesting contradiction has developed in the case of E.U. countries enforcing citizens' right of privacy; because privacy protections are ingrained in both the constitutional history and statutory frameworks of the European Union to a greater extent than in the United States,[240] the European Union has adopted a decidedly aggressive jurisdiction posture with regard to Internet data collections. According to some E.U. statements, the mere dropping of one cookie on an E.U. user hard-drive constitutes consent to jurisdiction in the European Union.[241] Thus, on the issue of data privacy litigation, the tables of litigiousness are inverted and the E.U. approach to Internet data privacy harms will generate a far greater volume of potential litigation than will the U.S. approach. Therefore, the Trusted Systems approach presents a compromise position of a jurisdiction framework based on a bright-line standard sensitive to data privacy concerns, but not necessarily resulting in a finding of jurisdiction in the forum of the plaintiff. As a result, in the context of allegations of intentional torts, such as privacy invasion, and intellectual property harms arising out of Network Communications, this approach may offer a workable middle ground and facilitate systemic integrity through creation of an integrated international Network Communications recourse structure.

Further, protecting U.S. citizens and the Network Communications space from trust erosion and infiltration mandates that we acknowledge that most Internet jurisdiction cases to date have not involved exclusively Internet contacts. Rather, both Internet and non-Internet contacts are involved in

237 *See, e.g.*, Silberman, *supra* note 235.
238 *Id.*
239 *See, e.g.*, Ronald A. Brand, *Comparative Forum Non Conveniens and the Hague Convention on Jurisdiction and Judgments*, 37 TEX. INT'L L.J. 467 (2002).
240 For a discussion of E.U. privacy regulation and how it differs from the U.S. approach to data privacy, see, for example, David Raj Nihawan, *The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States*, 56 VAND. L. REV. 939 (2003).
241 Juliana Gruenwald, European Privacy Laws Across the Pacific, http://www.zdnetindia.com/techzone/trends/stories/433.html (Nov. 6, 2000).

the assessment of whether an adequate basis for jurisdiction exists.

Consequently, crafting a coherent jurisdiction regime in the United States requires that, while it is essential to construct workable jurisdiction frameworks for Network Communications disputes, we must simultaneously remain sensitive to previous jurisdictional doctrine and carefully frame such new standards within the context of existing doctrine. It is only through such a careful approach that we can maintain the integrity and coherence of U.S. jurisdiction determinations as a whole. In adopting such an approach, I disagree with Professor Stein's assertion that no unique Internet frameworks are necessary;[242] as a society, we have already acknowledged statutorily that the Internet presents some unique problems that do not fall within the purview of existing statutory frameworks.[243] Certain jurisdictional determinations necessitate a medium-specific inquiry. However, I agree with the broader spirit of his message, which reminds us to be careful of and respectful of existing jurisdiction precedent and context. Professor Geist is correct in identifying data exchange as a component of the jurisdictional inquiry. I go further; I believe it is actually the critical component in determining whether a content provider has consented to jurisdiction in a particular forum and formed a relationship with a critical mass of citizens. However, I disagree with Professor Geist's advocacy of intellectually grounding an Internet jurisdiction inquiry in an effects test/targeting analysis arising out of *Calder*. As such, I agree more closely with Professor Redish's approach, though differ with him regarding the role of meaningful procedural inconvenience of the defendant as the sole, definitive constitutional inquiry.[244] Instead of viewing meaningful procedural inconvenience as the determinative inquiry,[245] I view the definitive inquiry to be whether there exists social responsibility and consent to jurisdiction on the part of the content provider as a consequence of data exchanges with a critical mass of users known to be citizens of a particular jurisdiction.

Finally, because the Trusted Systems approach to jurisdiction is premised on a paradigm of cooperative self-disclosure and mutual agency, it provides a technology neutral approach that will better promote systemic integrity on a long-term basis because it is less likely to be rendered obsolete by future technological advancements. Simultaneously, the approach attempts to encourage a sense of social responsibility and fair play in content providers. It facilitates a systemic reconceptualization of the role of data privacy and security concerns, reflecting a national recognition of the importance of data privacy. This recognition has already been evidenced by

242 *See* Stein, *Jurisdiction in Cyberspace*, *supra* note 2.
243 Examples of such an acknowledgment include the passage of the Children's Online Protection Act, 47 U.S.C. § 231, the Children's Online Privacy Protection Act, 15 U.S.C. § 6503, and the Children's Internet Protection Act, 114 Stat. 2763A-335, and the repeated introduction and passage of legislation addressing unsolicited email.
244 Redish, *supra* note 2.
245 *See id.*

the passage of the Gramm-Leach-Bliley Act[246] and the Health Insurance Portability and Accountability Act.[247] This trusted system paradigm recognizes the evolution of our economic system and the development of a market in consumer information; it also offers a jurisdiction approach sensitive to the organization of the network conveying such data.

CONCLUSION: THE IMPORTANCE OF ORGANIZATIONAL CODE

In this Article, I proposed an alternative framework for jurisdictional inquiries in cases alleging intentional torts or intellectual property harms arising out of Network Communications. This framework, which I call the Trusted Systems approach, is intellectually rooted in consent and social responsibility, and, as such, it incorporates both contractarian and regulatory jurisdictional approaches. The approach is operationalized through a bright-line calculation of known users within a particular jurisdiction and is sensitive to the different sizes of audiences controlled by different Network Communications content providers.

Unlike the sliding scale approach, which focuses analysis on the undefinable construct of website "interactivity," or the effects/targeting test, which also provides no coherent basis from which content providers can extrapolate to limit their liability, the Trusted Systems approach focuses its analysis on the quantified existence of social responsibility and consent to jurisdiction. Unlike the approach of the European Union, jurisdiction is not automatic in the jurisdiction of the plaintiff. Instead, the Trusted Systems approach asserts that, as a consequence of obtaining benefits from access to a critical mass of citizens within a particular jurisdiction, a content provider consents to jurisdiction in that forum.

Perhaps more importantly, the jurisdictional inquiry highlights a fundamental systemic question regarding our future approaches to regulation of Network Communications: are we approaching questions from an inappropriate regulatory paradigm? Perhaps we are still missing parts, critical parts, of the theoretical regulatory calculus. One such critical component, I would argue, is adequate consideration of the social and natural structures of organization that develop at the intersection of groups, strategic behaviors, and networks. These structures arise as a consequence of strategic behavior, but not necessarily by human design. A technologically-mediated communication network is not a *tabula rasa* bereft of organizational order. The incursion of law into the governance space of Network Communications must be informed by and considerate of the fundamental properties of the aggregate organizational order already in place, as well as the influence of content providers' legal strategy on the network's development. Network Communications regulation is destined for circumvention if it is di-

246 15 U.S.C.A. §§ 6801-09 (1999).
247 Pub. L. No. 104-191, 110 Stat. 1936 (1996).

vorced from these comparative economic and structural realities of the network.

To expand on a thoughtful taxonomy created by Lessig[248] and perhaps expanded by Benkler,[249] these hierarchies of organizational order might be termed "Organizational Code." Organizational Code includes the behavioral strategic norms of end users in the aggregate, those of entities doing business using the network and the legal norms of the technology transactions bar in shaping the comparative power and the legal strategies[250] of actors within the network. Thus, I submit that, in addition to being cognizant of the governing power of computer code and law, what Lessig calls "West Coast Code"[251] and "East Coast Code,"[252] respectively, and Benkler's addition regarding the importance of law and technology as a means of governments' unilateral encoding of values as behavioral constraints,[253] what might be called "Value Code," we must also pay attention to the "Organizational Code" of networks. We accomplish this by empirically and normatively studying the impacts of organizational structure and behavior on network structure and vice versa. Organizational Code develops at the intersection

248 LESSIG, *supra* note 30, at 5. In *Code*, Lessig argues that computer code, which he terms "West Coast Code," is an architecture of control and a powerful source of social regulation. A corollary statement that follows, therefore, is that any legal Internet regulation, or "East Coast Code," which ignores the influence of computer code as a social determinant is destined for impotence. *See also* Gordon Pask, *The Architectural Relevance of Cybernetics*, ARCHITECTURAL DESIGN 9/69 (1969) ("[R]apid advances will be made in . . . a proper and systematic formulation of the sense in which architecture acts as a social control.").

249 Benkler argues that regulation of information flows by governments are conducted within the framework of a dynamic relationship among this regulation, law, and technology. As such, unilateral Internet regulation by governments inherently results in systemic, cross-border repercussions because it encodes certain social values as behavioral constraints on users both inside and outside borders. Yochai Benkler, *Internet Regulation: A Case Study in the Problem of Unilateralism*, 11 EJIL 171, 177 (2000).

250 By legal strategy, I mean the pattern of organized legal approaches throughout an organization that are intended to strategically leverage legal structures in order to maximize competitive advantage and minimize liability, either on a proactive or emergent basis.

251 LESSIG, *supra* note 30, at 53–56.

252 Lessig's definition of East Coast Code is a decidedly regulatory and litigation-oriented perspective. Relational technology transactions legal norms sometimes drive the restructuring of physical network structure or the GUI of websites in advance of any regulatory or litigation guidance. Technology transactions counsel strive to enable entities to limit liability and plan for future business activities with certainty. Perhaps unlike norms in the world of litigation, where norms are determined to a certain extent by court rules and judicial preferences, transactional legal norms, though influenced by case law and regulation, evolve out of customs and habits of transactional behavior and through official and unofficial legal social networks. Many transactional norms do not result in litigation and thus their existence and nature is not necessarily well known by individuals outside the technology transactions bar.

253 Benkler's perspective contemplates formalized sources of legal regulation by a state within the international system, its patent and latent value transmission, and the resulting multilateral behavioral effects. Benkler, *supra* note 249, at 177. An Organizational Code perspective, instead, does not involve regulation as a starting point in its analysis. It begins with preexisting organizational structures within society and examines the economic behaviors of groups and their influence on comparative power within network structures. Following this analysis, the viability and appropriateness of regulatory intervention in lieu of private ordering can then be successfully addressed.

of network technology, law, and business strategy; it has and will continue to shape the regulatory landscape of networks in an integral and frequently invisible manner. As such, the preceding inquiry into Network Communications jurisdiction attempted to analyze the dynamics of jurisdictional determinations and standards through the lens of Organizational Code. Ultimately, although any interjection of law into Network Communications is fraught with risk, such interjection is essential. For better or worse, the days of Network Communications governed solely through private ordering are gone. In order to preserve the balance of economic and social interests embodied in the innovation policy of the United States, legal architectures must dovetail with technological architectures. They must also be conscious of and adapt in tandem with the evolution of conduct and structure in networks.