The Columbia
SCIENCE AND TECHNOLOGY LAW REVIEW
www.stlr.org

SOCIAL INTERMEDIARIES: CREATING A MORE RESPONSIBLE WEB THROUGH PORTABLE IDENTITY, CROSS-WEB REPUTATION, AND CODE-BACKED NORMS

Daniel H. Kahn[1]

Currently, our identities are scattered across the Web. At each website on which we participate, we must create new user names, personal profiles, social connections, and histories of activity. Without portable identities, we cannot fully reap the benefits of the emerging reputation economy. Moreover, because of the Web's structural limitations on identity, norm-based social governance has not played a significant role on most sites. The paucity of norms has created an atmosphere in which abusive behavior is common, heightening the apparent need for new legal regulation.

However, new tools, which I term social intermediaries, are poised to introduce portable identity to the Web. By allowing users to aggregate records of their activities across multiple sites, these tools increase reputation-based incentives for production. They also promote an atmosphere of respect by encouraging people to recognize each other as fully rounded individuals. Most importantly, they will allow many more sites to offer opportunities for users to govern each other through code-backed norms. This new opportunity for bottom-up social governance will help responsible users and site operators ameliorate the problems of abusive behavior on the Web. While social intermediaries introduce new regulatory challenges, their norm-building capacity shows that law is not the only answer to the Web's social problems.

[1] Law clerk to Judge James Robertson, U.S. District Court for the District of Columbia; Harvard Law School Post-Graduate Research Fellow. J.D. *cum laude*, Harvard Law School 2008; B.A. with Honors in Political Science, Yale College 2005. Thank you to Jonathan Zittrain for his invaluable assistance.

Cite as http://www.stlr.org/cite.cgi?volume=11&article=7

I. Introduction

When engineers designed what would eventually become the Internet, they chose not to build a system of identification into the inner workings of the network.[2] Their choice remains the status quo today: while Internet users must regularly provide various forms of self-identification to engage with websites, email clients, and other sources of online content, the infrastructure layers at the core of the Internet have no system to correlate identity to action.[3] As a result, there is not any centralized system to transport information about our identities between sites on the World Wide Web.[4]

Until recently, this proved to be an impassible barrier for identity; each site that allows participation has been forced to maintain its own user-identification system. Similarly, without portable identities on the Web, we must build new self-representations at each site on which we participate.[5] The self-descriptions, social connections, and histories of activity we develop on these sites are in a very real sense our Web "selves." The ability to construct multiple Web selves undoubtedly facilitates expression and can protect privacy. However, the absence of infrastructure to transport identity information means that we have to develop our identities anew at each site on which we participate, even if we might wish to employ a unified identity across multiple sites.

[2] *See* Jonathan Zittrain, The Future of the Internet and How to Stop It 31–33 (2008); David R. Johnson, Susan P. Crawford & John G. Palfrey, Jr., *The Accountable Internet: Peer Production of Internet Governance*, 9 Va. J. L. & Tech. 9, ¶ 82 (2004), http://www.vjolt.net/vol9/issue3/v9i3_a09-Palfrey.pdf. This choice is one manifestation of the "end-to-end" principle around which the Internet was designed. *See* Zittrain, *supra*, at 31–33.

[3] Engineers describe the Internet as consisting of several conceptual "layers" of network architecture. *See, e.g.*, Zittrain, *supra* note 2, at 67–69; Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law* 3 (Univ. of San Diego Sch. of Law Pub. Law and Legal Theory, Research Paper No. 55, 2003), *available at* http://ssrn.com/abstract=416263. While the exact characterizations vary, I will use the following (extremely simplified) model: (1) the "infrastructure" layers, through which data is transmitted; (2) the "application" layer, which represents the software that facilitates individual tasks; (3) the "content" layer, which comprises the actual information exchanged by users; and (4) the "social" layer, which describes the human interaction that overlays data exchange. What I term the infrastructure layers are typically described separately and include both hardware and software components. *See, e.g.*, *id.* at 3.

[4] The Web and the Internet are not synonyms. The Web is only a subset of the Internet. The latter also includes functions like Internet gaming and non-Web-based email. *See* Preston Gralla, How the Internet Works 116 (4th ed. 1998). I focus on the Web specifically, rather than the entire Internet.

[5] *See* Joseph Smarr, Plaxo, Google I/O 2008: OpenSocial, OpenID, and OAuth: Oh, My! (June 9, 2008), http://www.youtube.com/watch?v=6SYnlH5FXz0 (discussing the difficulty of transferring personal data between sites and stating "every single site acts like you've never used another website before in your life"); Pluck, White Paper: Social Bridging 1–3 (2010), http://www.pluck.com/learn/Pluck_Social_Bridging.pdf (analogizing the Web to a series of "islands" of isolated socializing).

In this Article, I explain how this disaggregation of identity harms Web users. First, it hinders participation in the emerging reputation economy. Second, it has rendered most sites inhospitable to bottom-up norm-driven governance.[6] Not surprisingly, the absence of constraining social forces has resulted in a flood of abusive behavior.[7]

Yet a new era of cross-Web identity is dawning. A few legal scholars have suggested that portable identity should be made possible through legal mandates[8] or through changes to the Internet's infrastructure layers.[9] However, I explain that new repositories of identity and reputational data are emerging at the Web's application layer.[10] These repositories, which I term "social intermediaries," are the cross-Web successors to social networking sites such as Facebook, MySpace, and LinkedIn.[11]

Most of the handful of legal academic writers who have mentioned social intermediaries thus far have done so only in passing.[12] These authors, and those who

[6] *See infra* Part IV.B–C.

[7] *See infra* Part III.A. Danielle Citron offers an excellent and disturbing primer on these concerns. *See* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. Rev. 61 (2009).

[8] *See, e.g.*, Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 Nw. U. L. Rev. Colloquy 1, 6–7 (2008), *available at* http://www.law.northwestern.edu/lawreview/colloquy/2008/25/LRColl2008n25Picker.pdf; *see also* Lilian Edwards & Ian Brown, *Data Control and Social Networking: Irreconcilable Ideas?*, *in* Harboring Data: Information Security, Law, and the Corporation 226-27 (Andrea Matwyshyn ed., 2009), *available at* http://ssrn.com/abstract=1148732 (suggesting value of legal protections for portable identity, but ultimately advocating "wait and see" approach).

[9] *See* Johnson et al., *supra* note 2 at ¶¶ 39-43 and 82-83 (suggesting that we may move voluntarily towards small networks built around portable identity that will eventually re-form into a new Internet); *see also* Ken D. Kumayama, Note, *A Right to Pseudonymity*, 51 Ariz. L. Rev. 427, 445-46, 462-63 (2009) (mentioning benefits of, but not explicitly advocating, architectural changes creating a new "identity layer" that would permit cross-Web pseudonymity).

[10] Social intermediaries are not verified identity systems, in which people must prove via credit cards or other means that they are who they claim to be. None of the tools I describe demand up-front proof of honesty in self-identification. *See infra* Part V.A.

[11] *See id.*

[12] *See* Jeffrey Aresty, *Digital Identity and the Lawyer's Role in Furthering Trusted Online Communities*, 38 U. Tol. L. Rev. 137, 149 (2006); Josh Blackman, *Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image Over the Internet*, 49 Santa Clara L. Rev. 313, 339–40 (2009); Molly Beutz Land, *Networked Activism*, 22 Harv. Hum. Rts. J. 205, 237 (2009); Viktor Mayer-Schonberger, *Virtual Heisenberg: The Limits of Virtual World Regulability*, 66 Wash. & Lee L. Rev. 1245, 1260 (2009); William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. Ill. L. Rev. 1105, 1121, 1161–62 (2009); Jane K. Winn, *Globalization and Standards: The Logic of Two-Level Games*, 5 J.L. & Pol'y for Info. Soc'y 185, 205 (2009). James Grimmelmann offers more meaningful analysis. *See* James Grimmelmann, *Saving*

ignore social intermediaries entirely, have vastly underestimated their importance and value for social ordering on the Web. Software developer Joseph Smarr states that social intermediaries are driving a transformation "as fundamental as the birth of the Web itself": the transformation to the "Social Web," meaning a move toward human interaction playing a more central role in Web use.[13] In this Article, I contend that social intermediaries will enable us to develop and deploy positive reputations across the Web, increasing the incentives to engage in socially valued behavior. Similarly, I argue that social intermediaries will promote a culture of respect by allowing Web users to recognize each other as rounded individuals worthy of respect and by exposing individuals to alternative points of view.

Most importantly, I argue that social intermediaries will decrease abusive behavior on the Web by facilitating norm development. Jonathan Zittrain expresses hope that innovative software can facilitate the development of "code-backed norms."[14] Similarly, Lior Strahilevitz writes of the possibility of "us[ing] technology to transform loose-knit environments, where reputation often fails to constrain antisocial behavior, into close-knit environments, where reputation constrains misbehavior more effectively."[15] Social intermediaries, I contend, are the technology to bring that transformation to the Web.[16] While the emerging Social Web creates new regulatory challenges, it also invites re-examination of calls for regulation that are premised on the absence of constraining social forces.

In late April 2010, Facebook brought the budding world of social intermediaries to the forefront for many of its users. With Facebook's newly introduced "Open Graph," users can employ the names and identity information contained in their Facebook accounts on numerous websites, allowing those sites to offer "instant personalization" of their features.[17] Existing Facebook users who sign in to Facebook and then visit

Facebook, 94 Iowa L. Rev. 1137, 1148, 1192–95 (2009).

[13] Joseph Smarr, Plaxo, Google I/O 2009: The Social Web: An Implementer's Guide (June 1, 2009), http://www.youtube.com/watch?v=juIko_o2ZWg.

[14] *See* Zittrain, *supra* note 2, at 223–28.

[15] Lior Jacob Strahilevitz, *"How's My Driving?" For Everyone (and Everything?)*, 81 N.Y.U. L. Rev. 1699, 1699 (2006).

[16] While I will discuss legal issues, my primary focus is on informal methods of governance. *Cf.* Jerry Kang, *Cyber Race*, 113 Harv. L. Rev. 1130, 1137–38 (2000) (focusing, in a discussion of racism and the Internet, primarily on social change rather than legal reform).

[17] *See* Posting of Alex Iskold to ReadWriteWeb, Facebook Open Graph: The Definitive Guide for Publishers, Users and Competitors, http://www.readwriteweb.com/archives/facebook_open_graph_the_definitive_guide_for_publishers_users_and_competitors.php (Apr. 23, 2010, 10:50 EST); Posting of Erick Schonfeld to TechCrunch, Zuckerberg: "We Are Building a Web Where the Default is Social", http://techcrunch.com/2010/04/21/zuckerbergs-buildin-web-default-social (Apr. 21, 2010). Facebook also has called its system simply "Facebook for Websites." *See* Facebook, Facebook for Websites, http://developers.facebook.com/docs/guides/web (last visited May 5, 2010).

participating third-party sites retain their Facebook identities by default, and they must actively "opt out" to avoid using Facebook's social intermediary features.[18] Whether intentionally or unwittingly, many Web users have had their first taste of portable identity and cross-Web social features via Facebook's new system.

Many users and even several U.S. Senators have criticized Facebook's Open Graph as a threat to privacy.[19] More generally, several legal scholars have implied that *all* social intermediaries threaten privacy.[20] Given the increased attention Facebook's recent changes have drawn to the issue, more discussion of social intermediaries' impact on privacy is surely forthcoming. I believe this is an important and worthwhile discussion, but privacy is not my focus here. My goal, instead, is to explore the under-appreciated and unique socio-legal benefits of social intermediaries. As privacy scholar Daniel Solove explains, there is a tension between reputation and responsibility, on the one hand, and privacy on the other.[21] This article focuses on the responsibility side of the

[18] *See* Facebook, *supra* note 17; Posting of Christina Warren to Mashable, Facebook Open Graph: What it Means for Privacy, http://mashable.com/2010/04/21/open-graph-privacy (Apr. 21, 2010).

[19] *See* Letter from Charles E. Schumer, U.S. Senator, et al., to Mark Zuckerberg, Facebook CEO, Apr. 27, 2010, *available at* http://www.politico.com/news/stories/0410/36406.html (criticizing "instant personalization" opt-out and encouraging Federal Trade Commission scrutiny); *see also,* e.g., Moveon.org, Petition: Facebook, Respect My Privacy!, http://www.facebook.com/group.php?gid=114387775262356 (last visited June 15, 2010) (presenting Facebook with petition with over 190,000 members asking to reverse its recent privacy policy changes). In response to the criticism, Facebook introduced simpler privacy controls, though it retained its opt-out policy. *See* Posting of Mark Zuckerberg to The Facebook Blog, Making Control Simple, http://blog.facebook.com/blog.php?post=391922327130 (May 26, 2010, 10:55 EST).

[20] *See* Blackman, *supra* note 12, at 339–40 (2009) (mentioning Facebook Connect as opening personal profile data to search engines in the context of a discussion highlighting new tools for "omniveillance"); McGeveran, *supra* note 12, at 1121, 1161-62 (discussing Facebook Connect and other portable identity software as potential new tools for social marketing, about which the author expresses privacy concerns). James Grimmelmann offers the most detailed and focused discussion of social intermediaries and privacy, arguing that portable identity threatens personal privacy by exposing personal data to unsecured websites. *See* Grimmelmann, *supra* note 12, at 1148 & n.53 (2009) ("If you asked me to pick the next Facebook feature to cause a massive privacy implosion, I'd guess Connect."); *id.* at 1192–95 (suggesting that "we should [] be extremely cautious about technical infrastructures for social network portability, like Google's OpenSocial, and APIs from MySpace and Facebook"). Note that "Facebook Connect" is the name for Facebook's earlier, slightly more privacy-protective social intermediary system, which was superseded by Open Graph. *See* Posting of Ben Parr to Mashable, Facebook to Kill Facebook Connect, http://mashable.com/2010/04/21/facebook-kills-facebook-connect (Apr. 21, 2010).

[21] *See* Daniel J. Solove, The Future of Reputation: Gossip, Rumor, and Privacy on the Internet 31–32 (2007), *available at* http://docs.law.gwu.edu/facweb/dsolove/Future-of-Reputation.

equation; its aim is to state the strongest case for social intermediaries as tools to empower Web users to govern themselves. While I recognize the importance of privacy, it is beyond the scope of this Article to weigh the benefits of social intermediaries against their potential privacy dangers.[22]

In Part II, I describe how identity and reputation are scattered on the non-intermediated Web.[23] In Part III, I examine leading problems at the Web's social layer, why site operators lack the incentives and tools to remedy them, and solutions proposed by legal scholars. In Part IV, I discuss norms as a strategy for governance, looking particularly at how some popular websites have used code-based norms successfully and why they have not taken hold on the Web at large. In Part V, I introduce social intermediaries, including both the backbone software for portable identity as well as user-facing tools like Facebook Open Graph and Google Friend Connect. In Part VI, I contend that portable identity and reputation will open the reputation economy to everyone and forward important legal values. In Part VII, I argue that social intermediaries will bring a new era of norm-based governance to the Web. In Part VIII, I look at some of the new challenges social intermediaries may introduce, including increased development of antisocial norms, new opportunities for invidious discrimination online, and over-enforcement of norms. In Part IX, I conclude that we should be guardedly optimistic about the growth of norms on the Social Web and that we should take these norms into account in determining when and how to regulate online social behavior.

II. Identity and Reputation on the Non-Intermedated Web

Countering prevalent "Wild West" imagery, Alfred C. Yen argues that the Internet is best analogized to feudal Europe.[24] While Yen focuses his analogy on domain names, ISP control of user activity, and copyright issues, his metaphor is also a good starting point for our understanding of identity and reputation on the non-intermediated Web. Just as feudal European kingdoms were fragmented into small and self-sufficient fiefs,[25] each website among the multitudes must maintain its own identity and reputation regime. This Part first explores how identity is confined to individual websites. It then

[22] The balance between privacy and responsibility must be struck at two levels—by individual users who choose whether and how to participate on social intermediaries, and by governing bodies, which may limit the outer bounds for social intermediaries' relationship with their users. Additionally, the weight of privacy threats may vary between social intermediary services, which may adopt more or less privacy-protecting systems and policies.

[23] By "non-intermediated Web," I mean the Web in the absence of social intermediaries. It describes both the historical period up until recently in which portable identity was unavailable and those portions of the Web today in which social intermediaries have not yet been adopted.

[24] *See generally* Alfred C. Yen, W*estern Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace*, 17 Berkeley Tech. L.J. 1207 (2002).

[25] *See id.* at 1232–36.

examines how that isolation locks average users out of the "Reputation Economy."

A. Scattered Identities and Reputations

Our Web identities and reputations are isolated into single-site containers. Most Web 2.0 sites[26] demand that we "log in" at the threshold of interactivity. If we wish to participate on a website, we must first create an account, typically consisting of a "user name" and password, to tie our actions to a persona.[27] We typically must create such new accounts at each separate site we use.[28] Even if an individual employs the same user name on multiple websites, it is unlikely that the name will be recognized by others from site to site given the massive number of Web participants.[29] Moreover, even if I happen to recognize a name on one site from its use on another, I cannot be certain the two names represent the same person.[30] "ABC123" on YouTube may not be "ABC123" on a Yahoo! forum.

Representing ourselves in our accounts with our "real names" and accurate photographs of ourselves cannot fully overcome this problem. Because instances of identity misrepresentation are common online,[31] even if we happen to recognize what appears to be the same user across multiple sites, we can rarely be sure that people are telling the truth about who they are. For instance, a trend developed in which the popular micro-blogging service Twitter became host to numerous impersonated celebrity accounts.[32]

[26] Web 2.0 sites are sites such as Flickr and YouTube that rely primarily on user-generated content. *See* Brandon Brown, Note, *Fortifying the Safe Harbors: Reevaluating the DMCA in a Web 2.0 World*, 23 Berkeley Tech. L.J. 437, 437 (2008).

[27] I use the term "account" to describe the basic credentials, such as a user name, an email address, and a graphic icon, by which users symbolize themselves to other users and to websites. In contrast, I use the term "identity" to mean "who a person is," more broadly. Unless otherwise noted, my use of "identity" can refer to either realistic online representations of offline self or more fanciful online self-representations.

[28] The situation is different on certain smaller networks of affiliated sites. For instance, an individual might use the same commenter name on the various Gawker Media blogs or on the various blogs hosted by LiveJournal.

[29] One source estimates that as of December 2009, over 1.7 billion people worldwide use the Internet in some fashion. *See* Internet World Stats, The Internet Big Picture: World Internet Users and Population Statistics, http://www.internetworldstats.com/stats.htm (last visited Apr. 15, 2010).

[30] *See* Smarr, *supra* note 5.

[31] *See, e.g.*, Solove, *supra* note 21, at 141 (describing impersonated legal celebrities).

[32] *See* Don Reisinger, *Top 10 Twitter Celebs: Real or Fake?*, CNET News, Apr. 15, 2009, http://news.cnet.com/8301-17939_109-10218926-2.html; Associated Press, *La Russa, Twitter*

Agency is therefore veiled; it is impossible to assert a single cross-Web identity reliably. Instead, our identities on the Web are radically disaggregated.[33] Moreover, we do not have any easy and reliable way to carry information about our hobbies, our personal relationships, or others' impressions of us from site to site. While many sites allow us to create personal profiles, these profiles do not make it simple for us to amalgamate information across sites. We also cannot easily transport information about our activity on one site onto another site. For instance, my profile on StubHub, a sports ticket resale site, does not tell users about the comments I have left in the hockey forums on ESPN.com. I might place a link on one site to my actions on the other, but this approach has limits. First, as discussed above, I could act deceptively. Second, this *ad hoc* method of linking cross-site activity does not scale; it might work to cross-link activities on a handful of sites, but not on a hundred.[34] In sum, on the non-intermediated Web, we have not had any "central banks" for identity or infrastructure to transport the personalities and reputation-building information we wish to compile.[35]

B. Cross-Web Isolation and the Reputation Economy

The term "reputation economy" has been used with two related meanings. First, it signifies that positive reputation can fuel economic gain.[36] This idea of reputation-as-means is captured by the common social science metaphor "social capital," used to illustrate that positive reputation and personal relationships have value, just like

Settle Lawsuit (June 5, 2009), http://sports.espn.go.com/mlb/news/story?id=4235409 (describing baseball manager Tony La Russa's settled lawsuit against Twitter over a user pretending to be him). In response to these problems, Twitter began verifying the identities of its most famous users. *See* Posting of Pete Cashmore to Mashable, Twitter Launches Verified Accounts, http://mashable.com/2009/06/11/twitter-verified-accounts-2 (Jun. 11, 2009). However, this solution is not available to all users. *See* Twitter, Verified Account, http://twitter.com/help/verified (last visited Apr. 4, 2010). Moreover, there is no reason to assume all sites will be as responsible as Twitter or have the resources to verify the offline identities of its users.

[33] Danielle Citron uses the term "disaggregat[ion]" to describe the separation between individuals' offline identities and their online personas. *See* Citron, *supra* note 7, at 63. While the online/offline disaggregation highlighted by Citron is undoubtedly important, it is online identities themselves that are far more scattered and "disaggregated."

[34] *See* Smarr, *supra* note 5.

[35] By "reputation," I mean third-party impressions of persons. *See* Oxford English Dictionary (2d ed. 1989) (2nd def.) (defining reputation as "[t]he common or general estimate of a person with respect to character or other qualities . . . ."). By "reputational data," "reputation-building data," and "reputational information," I use the accumulated information commonly used to build those third-party impressions.

[36] *See* Chris Anderson, The Long Tail: Why the Future of Business is Selling Less of More 76 (2006) ("Measured by the amount of attention a product attracts, reputation can be converted into other things of value: jobs, tenure, audiences, and lucrative offers of all sorts.").

conventional capital.[37] Attention is a scarce resource, and whoever captures it can gain in the reputation economy.[38] Second, "reputation economy" signifies that people compete for renown alone without regard for potential economic gain. For instance, open-source advocates explain how programmers are motivated to develop software for free by the possibility of increased esteem among fellow programmers.[39] Similarly, in his article advocating the adjustment of copyright law to give attribution a more prominent role, Greg Lastowka explores how software coders, fan-fiction authors, law professors, and French chefs all work to build reputations even though their behavior is not closely correlated with economic gain.[40]

Chris Anderson, the editor-in-chief of *Wired* magazine, touted the benefits of the emerging reputation economy during an interview with news satirist Stephen Colbert.[41] Anderson told Colbert that, while the possibility of monetizing reputation had always existed, "now that we're doing everything online," we are seeing the rise of "huge global reputation economies."[42] As an example of using the Internet to build reputation, Anderson told Colbert that he had 13,649 "followers" on Twitter who could read his updates regularly.[43] Colbert, in character as an egomaniac, responded, "Bite it! I've got half a million [followers]! Now, in the reputation economy, I'm way richer than you,

[37] *See* Robert D. Putnam, Bowling Alone: The Collapse and Revival of American Community 19–24 (2000) (explaining the concept of social capital); Nicole B. Ellison et al., *The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites*, 12 J. Computer-Mediated Comm., iss. 4, art. 1 (2007), *available at* http://jcmc.indiana.edu/vol12/issue4/ellison.html (summarizing research on benefits of social capital). More specifically, Chris Anderson refers to "reputation credits" or "attention credits." *See* Anderson, *supra* note 36, at 21, 163; *see also* Cory Doctorow, Down and Out in the Magic Kingdom (2003), *available at* http://craphound.com/down/download.php (describing a fictional post-scarcity society in which reputation is represented by a form of currency called the "whuffie").

[38] *See* Anderson, *supra* note 36, at 211; Picker, *supra* note 8, at 4 ("With the ready ability [online] to match advertising with content, a platform that generates pageviews is a valuable media property.").

[39] *See* Eric S. Raymond, The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary 79–136 (1999); Yochai Benkler, *Coase's Penguin, or, Linux and The Nature of the Firm*, 112 Yale L.J. 369, 426–34 (2002).

[40] *See* Greg Lastowka, *Digital Attribution: Copyright and the Right to Credit*, 87 B.U. L. Rev. 41, 59–62 (2007).

[41] *See The Colbert Report* (Comedy Central television broadcast July 22, 2009), *available at* http://www.colbertnation.com/the-colbert-report-videos/239500/july-22-2009/chris-anderson.

[42] *See id.*

[43] *See id.*

right?"[44]

Colbert *is* right, of course. Success in the reputation economy, whether defined in terms of monetary income or other more intrinsic rewards, rests in significant part on the level of attention we receive for our work. If our efforts to gain attention succeed, we might be able to sell advertising, grow in esteem among our peers, earn tenure, or feel pride in our success. The ability to garner attention turns on many factors, including talent, luck, and effort. Yet without an easy method to tie our works together or the reliable ability to clearly proclaim them as our own, it is difficult to build the kind of track record of quality that can draw consistent attention.

The Web should create a level playing field in which everyone can compete with Stephen Colbert the television star and Chris Anderson the magazine editor for "reputation riches." And to a significant extent, it has—but the revolution is not complete. Offline, there are pragmatic limits on the ability of reputation to scale—for instance, we can only remember a limited number of people. Online, software could overcome this limitation by providing potentially unlimited digital databases of reputational information. However, on the non-intermediated Web, we cannot easily amalgamate our online activities to achieve cross-Web recognition.

For those who seek Web-based "reputation riches," the main barrier to success is the difficulty in building trust. The threat of imitation and identity theft always looms. David Johnson, Susan Crawford, and John Palfrey underline this problem when they criticize the failure to build identity into the Internet's infrastructure layers.[45] They write that the lack of identity online "runs counter to the most fundamental needs of our social systems" because "[w]e cannot trust each other unless we know whom we are trusting."[46] A celebrity like Colbert can survive imitators thanks to his ability to draw attention to his real activity (Colbert himself has had over a dozen Twitter imitators, including one who accrued over 350,000 followers, competing with his real account).[47] Those who do not have access to especially trusted media sources (whether in traditional media or online) cannot overcome deception so easily.[48] While the Web is often described as "democratizing fame,"[49] the tenuous nature of identity online means that the playing field

[44] *See id.*

[45] *See* Johnson et al., *supra* note 2, at ¶ 83.

[46] *Id.*

[47] *See* Reisinger, *supra* note 32; *see also* Stephen Colbert on Twitter, http://twitter.com/stephencolbert (last visited Apr. 15, 2010) (most popular fake); Stephen on Twitter, http://twitter.com/stephenathome (last visited Apr. 15, 2010) (real).

[48] *Cf.* Citron, *supra* note 7, at 104 (suggesting that defamation cannot be cured through self-help because some people will not see the victim's response or believe it).

[49] *See, e.g.*, Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 Harv. J.L. & Tech. 1, 29 (2007); Lakshmi Chaudhry, *Mirror, Mirror on the Web*, *available at* The Nation, Jan. 29, 2007, at 19, http://www.thenation.com/doc/20070129/chaudry; Sarah Hinchliff, *Privacy and the Democratization of Fame*, Stanford Center for Internet and Society, July 9, 2009,

is not so level as the phrase suggests.

It is not only the would-be famous who suffer from the difficulty in amalgamating reputational information across websites. Sellers on eBay who have positive, established reputations on the site can sell at a premium compared to those who lack such reputations.[50] Yet Web users who have proven reliable transactors on one site cannot readily leverage their reputations in order to gain premiums on another site. Similarly, a user who builds a strong track record of quality comments on one site cannot easily point to that history in attempting to establish credibility on another site. As Danielle Citron notes, "[a]n individual must establish an online presence and begin to build an online reputation before aggregating ideas or economic opportunities with others online."[51] Without reliable account interconnection, establishing a meaningful presence is especially difficult for relatively casual, low-output Web users.

Moreover, content consumers are also harmed by reputation isolation. People often know nothing about the sources of information they consume on the Web. This lack of source information can lead to abuses. For instance, "astroturfing" refers to the common phenomenon of a small number of individuals or a commercial or political entity pretending to represent a broad-based "grassroots" movement.[52] The lack of identity information available about the "astroturfers" enables the deception.

To restate, most Web users do not have full access to the reputation economy. The majority of people cannot readily build recognizable cross-Web reputations. The few who succeed in gaining especially great popularity might reach the point where their names are recognized across multiple sites. Even these lucky and diligent few run the risk of impersonation and identity theft. The analogy of social capital reveals the inefficiency of reputation isolation.

III. Problems at the Web's Social Layer

This Part looks at the growing problems at the Web's social layer in order to examine the sphere in which the solutions offered by social intermediaries would operate. First, it summarizes the growing concerns about corrosive behavior on the Web. Next, it shows that site operators lack legal incentives to prevent abusive behavior. It also explains that even if liability for third-party content were expanded, moderation is often too time-consuming and difficult for individual site operators to undertake. Finally, it explores various approaches proposed by legal scholars to these difficult problems.

http://cyberlaw.stanford.edu/node/6220.

[50] *See* Tamar Frankel, *Trusting and Non-Trusting on the Internet*, 81 B.U. L. Rev. 457, 471 (2001); Cynthia G. McDonald & V. Carlos Slawson, Jr., Reputation in an Internet Auction Model, http://ssrn.com/abstract=207448 (Jan. 25, 2000); *see also infra* notes 141-145 (describing eBay's reputation system).

[51] Citron, *supra* note 7, at 68.

[52] *See* Wikipedia, Astroturfing, http://en.wikipedia.org/wiki/Astroturfing (last visited Apr. 15, 2010).

A. Social-Layer Problems

While Web 2.0 functionality allows new opportunities for user participation, it also expands opportunities for negative user behavior.[53] Such behavior is illustrated in the jargon of Internet culture: a "troll" refers to someone who intentionally engages in disruptive behavior characterized by abusiveness to other Web users;[54] "flaming" is the practice of excoriating another user, and a "flam[e] war" occurs when two or more users flame each other repeatedly.[55] Danielle Citron and other scholars have highlighted the frequency of defamatory, harassing, threatening, and other hateful communications on the Web.[56] The harms flowing from abusive speech on the Web are often greater than those from abusive speech offline because Web postings can reach anyone in the world, can last forever, and can be repeated easily. Citron refers to the ability of swarms of users to forward messages rapidly as the "aggregating" nature of the Internet.[57]

The Web has been praised as a place where people can communicate without being judged by physical characteristics.[58] Contrary to this idealized vision, Citron shows that groups such as women and minorities that have been traditional targets of discrimination offline have been singled out as targets of abusive behavior on the Web as well.[59] For instance, she documents how an anonymous mob wrote harassing blog posts and emails directed to programmer and technology blogger Kathy Sierra, including death

[53] Characterizing threatening online communications in the First Amendment action/expression rubric poses challenges. *See* Citron, *supra* note 7, at 100–01. By using the term "behavior," I do not mean to endorse any particular view.

[54] *See* Mattathias Schwartz, *Malwebolence*, N.Y. Times, Aug. 3, 2008, (Magazine), at 24 ("In the late 1980s, Internet users adopted the word 'troll' to denote someone who intentionally disrupts online communities.").

[55] *See* Diane Rowland, *Griping, Bitching and Speaking Your Mind: Defamation and Free Expression on the Internet*, 110 Penn St. L. Rev. 519, 520 (2006).

[56] *See, e.g.*, Citron, *supra* note 7, at 64–66, 69–81 (collecting stories and sources of statistics); Shira Auerbach, Note, *Screening Out Cyberbullying: Remedies for Victims on the Internet Playground*, 30 Cardozo L. Rev. 1641, 1641–45 (2009).

[57] *See id.*

[58] Peter Steiner's cartoon in the *New Yorker*, in which one dog sitting at a computer tells another dog that "on the Internet, nobody knows you're a dog," has gained widespread fame as a symbol of Internet privacy and anonymity. *See* Peter Steiner, *Cartoon*, The New Yorker, July 5, 1993, at 61, *available at* http://www.unc.edu/depts/jomc/academics/dri/idog.html; Glenn Fleishman, *Cartoon Captures the Spirit of the Internet*, N.Y. Times, Dec. 14, 2000, at G8 (describing fame and profitability of Steiner's cartoon).

[59] *See* Citron, *supra* note 7, at 69–81 (collecting sources); *see also* Kang, *supra* note 16, at 1135 ("[R]ace and racism are already in cyberspace.").

threats and an image of Sierra next to a noose.[60] As a result of the attacks, Sierra quit blogging and canceled a number of speaking engagements.[61] Similarly, in 2007, the message board AutoAdmit was home to a series of threatening, harassing, and intrusive comments about female law students at numerous schools.[62] These messages included an assertion hoping that one female Yale Law student would "get[] raped and die[]" and another claiming that she had a sexually transmitted disease.[63] Attackers also attempted to ensure their behavior would reach beyond the single site by engaging in "Google-bombing" so that the offensive threads would be prominent in Google searches for the female students' names.[64]

Less malicious but also disheartening is what Neil Netanel characterizes as the "flame-ridden cacophony" of discourse on the Web.[65] A great deal of user-generated content on the Web is inane and petty, and it often runs the risk of drowning out more valuable speech.[66] In addition to genuine user-generated content, "spambots" spew out advertisements disguised as blog comments and message board postings.[67] Tools including search engines, social bookmarking, and link-sharing features on social networks are designed to help Web users separate the wheat from the chaff. Yet the quantity of low-value discourse creates real costs in effort for consumers looking for higher-quality content. It also discourages participation by those who fear their

[60] *See* Citron, *supra* note 7, at 64–65.

[61] *Id* at 65.

[62] *See* Citron, *supra* note 7, at 71–75 (describing the attacks); Citizens Media Law Project, AutoAdmit, http://www.citmedialaw.org/threats/autoadmit (last visited Apr. 15, 2010) (history of the now-settled litigation).

[63] *See Doe v. Individuals*, 561 F. Supp. 2d 249, 251 (D. Conn. 2008).

[64] *See* Citron, *supra* note 7, at 73–74.

[65] Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 Cal. L. Rev. 395, 432 (2000).

[66] This point has been made far too strongly at times. *See, e.g.*, Mark Helprin, Digital Barbarism: A Writer's Manifesto *passim* (2009) (mocking the "mouth-breathing morons in backwards baseball caps" online); Andrew Keen, The Cult of the Amateur: How Today's Internet is Killing Our Culture *passim* (2007) (suggesting the Web is full of "user-generated nonsense" that drowns out high-quality, professional work). Nevertheless, even those who embrace the Internet's freedom need only visit an unmoderated message board to concede the low quality of a significant amount of Internet discourse.

[67] *See, e.g.*, Lessig Blog, Announcing the Hibernation of Lessig.org/blog, http://lessig.org/blog/2009/08/announcing_the_hibernation_of.html (Aug. 20, 2009, 2:15 EST) (announcing a sabbatical from blogging, in part because over one-third of the 30,000 comments posted to his site came from "fraudsters," including spambots advertising online casinos).

contributions might be lost amid the cacophony.[68]

Another growing problem at the Web's social layer is what Jonathan Zittrain terms "privacy 2.0."[69] "Privacy 2.0" issues originate in Web 2.0 user-generated content and emanate from individual to individual rather than from governments or large corporations, as with more traditional privacy problems.[70] The story of "Star Wars Kid" is illustrative of privacy 2.0 concerns. In 2002, a French Canadian high school student was videotaped pretending to swing a golf ball retriever like a lightsaber from *Star Wars*.[71] Several of the student's classmates found the video and put it online.[72] By November of 2006, a marketing agency estimated that the video had been viewed 900 million times.[73] All of these viewings were without the consent of "Star Wars Kid" himself, who was upset with the experience and filed suit against his classmates who had first released the video.[74]

B. Section 230 and the Failure of Site Operators to Manage Social Layer Problems

Social-layer problems could be mitigated by site operators, who control the content on their sites. Yet this Sub-Part will show that they have lacked legal incentives and technical capacity to tackle these problems.

In the United States, the law permits site operators freedom in choosing whether to moderate user-generated content.[75] In *Stratton Oakmont, Inc. v. Prodigy Services Co.*, a New York court held Prodigy, an early online service provider, liable for defamatory

[68] *See, e.g.*, Patrick Leary et al., *Free Speech, Quality Control, and Flame Wars*, Academe, Jan.-Feb. 2007, http://www.aaup.org/AAUP/pubsres/academe/2007/JF/Feat/Lear.htm (describing, *inter alia*, efforts to put out flame wars on academic mailing lists in order to prevent quality contributors from leaving); Posting of Orin Kerr to The Volokh Conspiracy, Developing a Comment Culture, http://volokh.com/posts/1233215010.shtml (Jan. 29, 2009, 2:43 EST) ("If a blogger doesn't moderate comment threads at all on a widely read blog, people who want to be shocking, mean, or just irrelevant realize they can do their thing and reach a decent-sized audience. They eventually push out the more thoughtful people . . . .").

[69] *See* Zittrain, *supra* note 2, at 205.

[70] *See id.*; *see also* Solove, *supra* note 21 (collecting stories throughout).

[71] *See* Helen A.S. Popkin, *Survive Your Inevitable Online Humiliation*, MSNBC.com, Sept. 6, 2007, http://www.msnbc.msn.com/id/20611439.

[72] *See id.*

[73] *See Star Wars Kid is Top Viral Video*, BBC News, Nov. 27, 2006, http://news.bbc.co.uk/2/hi/entertainment/6187554.stm.

[74] *See* Popkin, *supra* note 71.

[75] While many of this Article's points can apply with equal force in other countries, my focus is on the United States and U.S. law.

statements posted by a third-party in its discussion forums.[76] The court found that because Prodigy moderated its forums, it took sufficient responsibility for their contents to be deemed the publisher of the defamatory quotes.[77] In 1996, Congress, unhappy with the *Stratton Oakmont* court's decision to punish Prodigy for moderating its forums,[78] passed the Communications Decency Act ("CDA").[79] One provision of the CDA, codified at 47 U.S.C. § 230 and commonly referred to as § 230, was designed to encourage "'Good Samaritan' blocking and screening of offensive material."[80] Section 230(c)(1) states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[81] Courts quickly interpreted § 230 as a broad barrier to liability for hosts of third-party content.[82] In addition, courts have construed "interactive computer service" broadly to include not only ISPs but also websites that host user-generated content.[83]

[76] *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, No. 31063/94, 1995 N.Y. Misc. LEXIS 229, at *10–14 (N.Y.S.2d May 26, 1995).

[77] *See id.*

[78] *See* 141 Cong. Rec. H 8469 (daily ed. Aug. 4, 1995) (statement of Rep. Cox); Ken S. Myers, *Wikimmunity: Fitting the Communications Decency Act to Wikipedia*, 20 Harv. J. L. & Tech, 163, 173 (2006).

[79] *See* Telecommunications Act of 1996, Pub. L. No. 104-104 tit. V, 110 Stat. 56, 133–43 (1996). The CDA is actually the short title for Title V of the larger Telecommunications Act of 1996, which overhauled telecommunications law. *See id.* § 501, 110 Stat. at 133.

[80] *See* 47 U.S.C. § 230(c) (2006).

[81] *See id.* § 230(c)(1).

[82] *See, e.g.*, *Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666, 669, 671–72 (7th Cir. 2008) (finding based on § 230 that a website could not be held liable under the Fair Housing Act, 42 U.S.C. § 3604(c) (2006), for third-party discriminatory housing advertisements); *Universal Commc'n Sys. v. Lycos, Inc.*, 478 F.3d 413, 419 (1st Cir. 2007) (finding a search engine immunized against liability for third-party postings); *Ben Ezra, Weinstein, & Co. v. Am. Online Inc.*, 206 F.3d 980, 983 (10th Cir. 2000) (finding AOL immunized against liability for third-party postings of allegedly inaccurate information on publicly traded stock); *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 328 (4th Cir. 1997) (finding AOL immunized against liability for allegedly defamatory third-party posting). *But cf. Fair Hous. Council v. Roommates.com, LLC*, 521 F.3d 1157, 1166-67 (9th Cir. 2008) (finding Roomates.com liable for third-party postings that violated the Fair Housing Act, based on the website's discriminatory questions and choices of answers for users); *Doe v. GTE Corp.*, 347 F.3d 655, 659–60 (7th Cir. 2003) (suggesting that § 230(c)(1) is "definitional" and thus not a barrier to liability where state law requires some standard of care for third parties).

[83] *See, e.g.*, *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1123 (9th Cir. 2003); *Lycos*, 478 F.3d at 419; *see also* 47 U.S.C. § 230(f)(2) (2006) (defining "interactive computer service" as "any information service, system, or access software provider that provides or enables

Notwithstanding Congress's goal, one result of § 230 is that site operators are free to ignore defamatory or otherwise tortious user-generated content on their sites.[84] Daniel Solove argues that § 230 contributes to an atmosphere in which site operators gladly welcome non-tortious but offensive content on their sites, eager for the attention such content can bring.[85] Therefore, Solove and others have called for § 230 to be reformed to open site operators to increased liability.[86]

Even those site operators who have wished to maintain minimum standards of quality for user participation have found it difficult to do so. On popular sites that inspire uncommon devotion from visitors, site operators can give dedicated volunteers tools to moderate fellow participants.[87] For site operators who cannot inspire volunteers, the alternatives are to hire moderators (for larger companies) or to moderate their own site (for hobbyists). Since top-down methods of regulating user activity online are time- and labor-intensive, neither strategy can be wholly effective. It would rarely make economic sense for professional operators of popular sites to hire enough employees to police all user-generated content. Similarly, thorough moderation would often demand too much time from hobbyists to be reasonable.

Illustrative of the strategies employed by hobbyist site operators are those used by bloggers in a small corner of the "blogosphere" likely to be especially familiar to readers—law professors' blogs. On many such sites, the bloggers delete comments they deem inappropriate and delete commenter accounts of repeat offenders.[88] Law professor

computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet"). Notably, at least one court has held that § 230 protects social networking sites. *See Doe v. MySpace*, Inc., 474 F. Supp. 2d 843, 848–50 (W.D. Tex. 2007).

[84] *See* Solove, *supra* note 21, at 153–59; Citron, *supra* note 7, at 118–19.

[85] Solove, *supra* note 21, at 159; *cf.* Susan Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 Harv. J.L. & Tech. 569, 629 (2001) (contending that, if pushed by threats of liability, companies would invest in technological solutions to defamation).

[86] *See* Solove, *supra* note 21, at 159; Citron, *supra* note 7, at 115–25. Others have called for increased liability for ISPs that fail to filter undesirable material. *See* Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 Sup. Ct. Econ. Rev. 221, 222–25 (2006); Matthew G. Jeweler, *The Communications Decency Act of 1996: Why § 230 is Outdated and Publisher Liability for Defamation Should be Reinstated Against Internet Service Providers*, 8 U. Pitt. J. Tech. L. & Pol'y 3 (2007); Mark A. Lemley, *Digital Rights Management: Rationalizing Internet Safe Harbors*, 6 J. Telecomm. & High Tech. L. 101, 115–18 (2007). Susan Freiwald has called for a more mixed approach. *See* Freiwald, *supra* note 85, at 643 (recommending comparative institutional analysis to determine when and where third-party liability is appropriate).

[87] *See infra* Parts IV.B & VII.B.3.

[88] *See, e.g.*, Discourse.net, Comments Policy Version 1.2, http://www.discourse.net/archives/2008/09/comments_policy_version_12.html (Sept. 12, 2008, 8:33 EST) (threatening deletion or "disemvowel[ment]" for policy violators); Kerr, *supra* note 68

Michael Froomkin has threatened to block the IP addresses of especially vitriolic commenters from his site.[89] An alternative to the *ex post* approach of deleting comments and commenters after the fact is an *ex ante*, or gatekeeping, approach.[90] For example, on OrinKerr.com, Professor Kerr only allowed comments to be displayed that he approved or that came from a pre-approved source he trusted.[91] Professors have expressed frustration at the amount of effort involved in moderating comments and at the obstinate nature of some malignant commenters.[92] As a result, some simply disallow all comments.[93] While by definition this final strategy always prevents unwanted user behavior, site operators must sacrifice all of the benefits of interactivity.

(stating heavy moderation is necessary for productive discussion); Lessig Blog, 37 Helpful Comments Later, http://lessig.org/blog/2008/05/37_helpful_comments_later.html (May 1, 2008, 21:58 EST) (stating author has started deleting personal attacks, having previously only deleted spam); Posting of Daniel Solove to Concurring Opinions, Our Comment Policy, http://www.concurringopinions.com/archives/2009/04/our_comment_pol.html (Apr. 19, 2009, 12:07 EST) (creating comment policy for group blog).

[89] *See* Froomkin, *supra* note 88. An "IP address" is a unique numerical designation for computers, devices, and networks connecting to the Internet. *See* Wikipedia, IP Address, http://en.wikipedia.org/wiki/IP_address (last visited Apr. 15, 2010). Blocking an IP address bans any device at that address from using a site. *See* Wikipedia, IP Blocking, http://en.wikipedia.org/wiki/IP_blocking (last visited Apr. 15, 2010).

[90] *See infra* Part VII.B (discussing these terms more).

[91] *See* OrinKerr.com, A Comment About Comments, http://www.orinkerr.com/2006/05/04/a-comment-about-comments (May 4, 2006, 16:07 EST); OrinKerr.com, Welcome—And a Comment on Comments, http://www.orinkerr.com/2006/03/13/welcome-and-a-comment-on-comments (Mar. 13, 2006, 00:15 EST).

[92] *See, e.g.*, Posting of David Bernstein to Volokh Conspiracy, My Comments Policy, http://www.volokh.com/posts/1250794848.shtml (Aug. 20, 2009, 15:00 EST) (stating the author will only leave comments open occasionally due to the effort involved in moderation); Posting of Orin Kerr to Volokh Conspiracy, Commenting About Commenting, http://volokh.com/posts/1229290087.shtml (Dec. 14, 2008, 16:28 EST) (expressing frustration at difficulty of moderation); Brian Leiter's Law School Reports, A Word on My Comments Policy, http://leiterlawschool.typepad.com/leiter/2008/10/a-word-on-my-co.html (Oct. 20, 2008, 3:03 EST) (stating that the authors opens comments only occasionally because doing it so is time-consuming).

[93] *See, e.g.*, Posting of Jack Balkin to Balkinization, New Comments Policy at Balkinization, http://balkin.blogspot.com/2009/01/new-comments-policy-at-balkinization.html (Jan. 29, 2009, 00:17 EST) (stating the Balkinization group blog will not allow comments unless an author requests them); Posting of Jack Balkin to Balkinization, Some Additional Notes on Comments and Social Software, http://balkin.blogspot.com/2009/01/some-additional-notes-on-comments-and.html (Jan. 29, 2009, 10:05 EST) [hereinafter Balkin Notes] (explaining why closing a comment section makes sense when moderation is difficult); Posting of Randy Barnett to Volokh Conspiracy, Comments Off, http://volokh.com/posts/1233607340.shtml (Feb. 2, 2009, 3:42 EST) (stating the author is "out there without comments and lovin' it").

In sum, although site operators could, in theory, restrict abusive user behavior, under the *status quo* it is simply not realistic to expect them to do so. Without legal incentives, site operators do not have to moderate, even in the face of tortious user behavior. Moreover, without sufficient technical tools, most site operators have been left with a choice between shutting down user participation or opening participation to both good and bad alike.[94]

C. Legal Scholars' Responses to Problems at the Social Layer

Lawrence Lessig describes four methods of controlling behavior online: law, code (or architecture), markets, and norms.[95] Responses in the legal literature to the problems at the Web's social layer can be divided into two groups: (1) those that advocate legal solutions, and (2) those that advocate "soft" solutions based on norms.[96] This Sub-Part will sketch each of these two approaches.

Some scholars, politicians, and others call for a position that Danielle Citron memorably terms "fundamentally pro-regulatory."[97] These advocates believe that existing regulations are insufficient to protect against abusive online behavior.[98] They are a part of a broader movement of writers who have pushed back against what they view as the "astringently libertarian" perspective that dominates Internet political culture.[99] While it is beyond the scope of this Article to catalogue these writers' proposals to regulate the Web's social layer, they include calls to do the following: expand or alter the scope of private civil causes of action against either tortfeasors directly[100] or against intermediaries,[101] increase the substantive scope of applicable

[94] *See* Balkin Notes, *supra* note 93 (stating that "[c]ode matters" in moderation ability).

[95] *See* Lawrence Lessig, Code 2.0 120–25 (2006).

[96] Suggestions in both categories interact with code and markets, but solutions based solely on code or markets would be incongruous in the legal literature.

[97] Citron, *supra* note 7, at 66; *see also infra* notes 100–04 and accompanying text.

[98] Citron provides a useful summary of existing tort and criminal law in the United States that could be used against abusive behavior online. S*ee* Citron, *supra* note 7, at 86–88.

[99] Putnam, *supra* note 37, at 173; *see also* Jack Goldsmith & Tim Wu, Who Controls the Internet: Illusions of a Borderless World 136–45 (2006); Lawrence Lessig, Code and Other Laws of Cyberspace 85-90 (1999); Cass R. Sunstein, Republic.com 2.0 111–12 (2007); Citron, *supra* note 7, at 66; Jay P. Kesan, *Private Internet Governance*, 35 Loy. U. Chi. L.J. 87, 90–93 (2003); Netanel, *supra* note 65; Jonathan Zittrain, *The Generative Internet*, 119 Harv. L. Rev. 1974 (2006).

[100] *See*, *e.g.*, Solove, *supra* note 21, at 186–87 (proposing expansion of the appropriation tort); Abril, *supra* note 49 (advocating altering privacy torts for "spaceless" online world); Citron, *supra* note 7 (suggesting expanded application of civil rights law in online context).

criminal law,[102] decrease procedural protections for anonymous online parties,[103] and mandate changes to code.[104]

In contrast, many scholars call for private responses to online social problems.[105] The Internet facilitates peer-production of goods and services.[106] Norms are distributed and peer-produced principles of behavior.[107] As a result, it should be no surprise that

[101] *See supra* note 82.

[102] *See, e.g.*, Alexander Tsesis, *Hate in Cyberspace: Regulating Hate Speech on the Internet*, 38 San Diego L. Rev. 817, 869–71 (2001). In 2006, teenager Megan Meier committed suicide after being provoked in a prank in which her neighbors pretended on MySpace to be a teenage boy who initially expressed romantic interest in Megan and then mocked her. *See* Sarah Jameson, *Cyberharrassment: Striking a Balance Between Free Speech and Privacy*, 17 CommLaw Conspectus 231, 231–32 (2008). Lori Drew, one of the neighbors who perpetrated the hoax, was prosecuted unsuccessfully in federal court. *See United States v. Drew*, 259 F.R.D. 449, 462–67 (C.D. Cal. 2009) (dismissing portion of indictment upon which Drew had been found guilty). Due to moral outrage at the case and concern that no law forbade Lori Drew's behavior, a number of anti-cyber-bullying laws have been proposed. *See* 2009 Tenn. Pub. Acts 347 (amending Tennessee harassment law to forbid some forms of cyberbullying; passed into law, Tenn. Code. Ann. § 39-17-308 (2009)); Megan Meier Cyberbullying Prevention Act, H.R. 1966, 111th Cong. (2009) (providing criminal fines or up to two years of imprisonment for "using electronic means to support severe, repeated, and hostile [harassing] behavior"); Jameson, *supra*, at 264-66 (advocating a federal criminal statute against cyberbullying).

[103] *See, e.g.*, Jameson, *supra* note 102, at 265-66 (calling for decreased anonymity to battle cyberbullying); Jason Miller, *Who's Exposing John Doe? Distinguishing Between Public and Private Figure Plaintiffs in Subpoenas to ISPs in Anonymous Online Defamation Suits*, 13 J. Tech. L. & Pol'y 229, 254–59 (2008) (advocating a lower standard for revealing the identities of defendants under subpoena where the plaintiff is a private figure); *infra* note 310 and accompanying text. Presently, most courts require some heightened proof from plaintiffs before they will allow subpoenas to be served on ISPs to unmask "John Doe" defendants. *See, e.g.*, *Doe v. Cahill*, 884 A.2d 451, 457 (Del. 2005); *Doe v. Individuals*, 561 F. Supp. 2d 249, 254 (D. Conn. 2008).

[104] *See, e.g.*, Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 Mich. L. Rev. 395 (1999) (arguing for a zoning system for the Internet); R. Polk Wagner, *Filters and the First Amendment*, 83 Minn. L. Rev. 755 (1999) (calling for site operators to be required to include easy-to-filter language in their sites' codes).

[105] Because norms shape and delimit the possibilities for human behavior, they can be conceived as a form of "governance." *See* Lessig, *supra* note 99, at 122, 124; Netanel, *supra* note 65, at 400.

[106] *See generally* Yochai Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedom 29–127 (2006).

[107] *See* Robert C. Ellickson, Order Without Law: How Neighbors Settle Disputes 127–31 (1991).

some cyber-scholars hope "peer production of governance"[108] and "netizenship" will flourish on Internet communities.[109] While it is widely agreed that private ordering plays a significant role on the Web,[110] these advocates hope to see it play a greater role.

Jonathan Zittrain expresses hope for "code-backed norms"—features embedded in websites or elsewhere on the Internet that enable users to develop and implement social governance.[111] Analogously, Lior Strahilevitz, in *How's My Driving? For Everyone and Everything*, proposes delegating traffic law enforcement to drivers by requiring placards on all automobiles to enable drivers to critique each other.[112] He suggests that systems comparable to his *How's My Driving* proposal could be deployed in other circumstances as well.[113] Strahilevitz's vision differs from Zittrain's in that the *How's My Driving* system would be government-mandated and backed by legal sanctions for oft-criticized drivers.[114]

Much of the remainder of this Article will focus on how social intermediaries promote the development of "code-backed norms" on the Web. I will argue that "soft" governance will play an increasing role on the Web in coming years and that this change should generally be welcomed. In doing so, I do not wish to rehash the old debate held at the dawn of the Internet's public ascendancy over whether law should generally defer to norms with regard to online governance.[115] Instead, I wish to make the more modest

[108] Johnson et al., *supra* note 2.

[109] *See* Zittrain, *supra* note 2, at 127–149, 168–74, 223–31 ("The ongoing success of enterprises like Wikipedia suggests that social problems can be met first with social solutions—aided by powerful technical tools—rather than by resorting to law."); I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. Pitt. L. Rev. 993, 1040–41, 1054 (1994) (contending that the presumption for governance online should be in favor of self-help and custom rather than legal enforcement); David R. Johnson, *The Life of the Law Online*, 51 N.Y.L. Sch. L. Rev. 956, 966–71 (2006) (calling for the "rise of netizenship"); Johnson et al., *supra* note 2 (suggesting that the Internet will become broken into smaller private communities of self-governance); David G. Post, *Governing Cyberspace*, 43 Wayne L. Rev. 155, 170–71 (1996) (arguing the Internet may help realize radical liberty of choice in governance).

[110] Even skeptics of online norms concede this much. *See* Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 Chi.-Kent L. Rev. 1257, 1260–61 (1998); Netanel, *supra* note 65, at 451–52, 498.

[111] *See* Zittrain, *supra* note 2, at 223–28.

[112] *See* Strahilevitz, *supra* note 15.

[113] *See id.* at 1759–65.

[114] *See id.* at 1717–19.

[115] The argument that private ordering online holds special normative value was often made in conjunction with the argument that jurisdictional issues render regulation of the Internet futile. *See, e.g.*, David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367, 1395–1400 (1996); Henry H. Perritt, Jr., *Cyberspace Self-Government: Town*

claim that we should account for the coming growth of norms in our decisions about when and how to regulate, as the new growth of norms may sometimes obviate (or occasionally exacerbate) the need for regulation.

IV. NORMS AND THE NON-INTERMEDIATED WEB

Consistent with this Article's focus on "soft" governance, this Part will first briefly review general scholarship on norms. It will then describe several websites that are widely cited as "code-backed norms" success stories. Finally, it will examine why norms have not yet flourished on most sites.

A. Norms Generally

Norms are privately created, implicit rules of behavior.[116] Study of the relationship between law, norms, and economics has burgeoned in recent years.[117] Legal scholars, drawing on social science literature and methodology, have investigated the role of norms in contexts ranging from ancient Athenian courts to modern American cotton producers.[118] As Cass Sunstein explains, "norm management is an important strategy for accomplishing the objectives of law."[119]

Jeffrey Rachlinski states that extensive social psychology research supports the following two propositions: (1) "groups develop and impose norms on their members," and (2) "the apparent behavior of others can alter the social meaning of a situation in ways that profoundly affect behavior."[120] In other words, norms influence our behavior

Hall Democracy or Rediscovered Royalism?, 12 Berkeley Tech. L.J. 413, 477–78 (1997). *But see* Goldsmith & Wu, *supra* note 99 (criticizing the view that jurisdictional challenges undermine the ability of sovereign states to regulate the Internet); Lemley, *supra* note 110 (contending that courts should not defer to online norms); Netanel, *supra* note 65 (arguing that legal regulation is superior to private ordering online based on liberal and democratic values).

[116] *See* Ellickson, *supra* note 107, at 127–31. Robert Ellickson defines norms as means of informal control based upon social forces that are enforced through vicarious self-help sanctions. *Id.* at 131.

[117] *See, e.g.*, *infra* notes 118–133.

[118] *See* Adriaan Lanni, *Social Norms in the Courts of Ancient Athens*, 1 J. Legal Analysis 691 (2009); Lisa Bernstein, *Private Commercial Law in the Cotton Industry: Creating Cooperation Through Rules, Norms, and Institutions*, 99 Mich. L. Rev. 1724 (2001). *See generally* Lanni, *supra*, at 691–92 (cataloging empirical norms research by law professors); Lemley, *supra* note 110, at 1261–62 (acknowledging the existence of such research).

[119] *See* Cass R. Sunstein, *Social Norms and Social Roles*, 96 Colum. L. Rev. 903, 907 (1996).

[120] Jeffrey J. Rachlinski, *The Limits of Social Norms*, 74 Chi.-Kent L. Rev. 1537, 1540

based both on external pressure from others and internalized desire to conform.[121] Norms must be understood in their cultural context; Lawrence Lessig offers the example of a nineteenth century caning victim who, because of the social injury involved, feels more hurt than the loser of a pistol duel.[122]

Norms play an important role in group membership and group formation.[123] Norms are most likely to emerge successfully in close-knit groups, which are "made up of repeat players who can identify one another"[124] and in which "power is broadly distributed among group members and the information pertinent to informal control circulates easily among them."[125] Homogeneity within groups promotes norm development as well, whether the homogeneity is based on shared traits or shared interests.[126]

Norms require significant community investment in enforcement. If there are too many defectors and enforcement is lacking, it is hard to say that a norm exists.[127] On the flip-side of enforcement, Dan Kahan explains that atmospheres of trust and reciprocity are key to norm creation.[128] He also contends, based on social science research, that regulatory incentives can actually undermine cooperation by focusing people's attention solely on self-interest.[129]

While norms are powerful, they are far more chaotic and less subject to

(2000).

[121] *See id.* at 1545–46 (describing various theories on how norms influence behavior). In contrast to this view, some law and economics scholars see norms only in terms of their relation to external motivation. *See* Eric Posner, Law and Social Norms 5, 11–27 (2002); Alex Geisinger, *Are Norms Efficient? Pluralistic Ignorance, Heuristics, and the Use of Norms as Private Regulation*, 57 Ala. L. Rev. 1, 7 (2005).

[122] *See* Lawrence Lessig, *Social Meaning and Social Norms*, 144 U. Pa. L. Rev. 2181, 2183 (1996).

[123] *See, e.g.*, Lisa Bernstein, *Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry*, 21 J. Legal Stud. 116, 134–35 (1992) (describing the diamond industry, in which group membership is valued over apparent contractual benefits).

[124] Lior Jacob Strahilevitz, *Social Norms from Close-Knit Groups to Loose-Knit Groups*, 70 U. Chi. L. Rev. 359, 359 (2003).

[125] Ellickson, *supra* note 107, at 177–78; *accord* Strahilevitz, *supra* note 124, at 359.

[126] *See* Daryl J. Levinson, *Collective Sanctions*, 56 Stan. L. Rev. 345, 375 (2003).

[127] *See* Lessig, *supra* note 122, at 2185.

[128] *See* Dan M. Kahan, *The Logic of Reciprocity: Trust, Collective Action, and Law*, 102 Mich. L. Rev. 71 (2003) (collecting social science research).

[129] *See id.* at 76–77; *see also* Jeffrey Rosen, *I-Commerce: Tocqueville, the Internet, and the Legalized Self*, 49 Drake L. Rev. 427, 427-28 (2001) (suggesting that an atmosphere of legalism can displace one of social norms).

government control than legal regulation.[130] First, norms can be hard to "aim." Predicting how people react in specific circumstances can be difficult, and multiple norms can conflict with one another.[131] Second, norms can compel socially harmful behavior. For example, in a series of experiments, psychologist Stanley Milgram used social pressure to induce students to give apparently severe electric shocks to strangers.[132] Finally, the ability of individuals to recognize norms and group preferences is limited by human cognitive biases.[133]

B. Norm Successes on the Web

Certain popular websites have successfully shaped user behavior through code-backed norms. This Sub-Part will briefly sketch the systems employed by the three sites that have been most widely praised in the legal literature as norm success stories: eBay,[134] Wikipedia,[135] and Slashdot.[136]

1. eBay

When buyers and sellers complete a transaction on eBay, the online auction site, they are encouraged to give feedback to the community on their partner in exchange.[137] Users can rate their experience as positive, neutral, or negative, and can leave text

[130] Nevertheless, law's expressive value can help to some degree to foster specific norms. *See* Lawrence Lessig, *The Regulation of Social Meaning*, 62 U. Chi. L. Rev. 943, 1008-14, 1044 (1995); *see also* Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 Mich. L. Rev. 373, 404, 407–14 (discussing law's use in establishing norms against online harassment of women).

[131] *See* Rachlinski, *supra* note 120, at 1566–67.

[132] *See id.* at 1556–62. *See generally* Stanley Milgram, Obedience to Authority (1974).

[133] *See* Geisinger, *supra* note 121, at 21–24.

[134] *See, e.g.*, Frankel, *supra* note 50, at 471; Picker, *supra* note 8, at 6–7; Rosen, *supra* note 129, at 435–36.

[135] *See, e.g.*, Zittrain, *supra* note 2, at 133–41; Myers, *supra* note 78, at 167–70.

[136] *See, e.g.*, Benkler, *supra* note 106, at 76–80; Benkler, *supra* note 39, at 393–96; A. Michael Froomkin, *Habermas@Discourse.Net: Toward a Critical Theory of Cyberspace*, 116 Harv. L. Rev. 749, 863–67 (2003); Rosen, *supra* note 129, at 436.

[137] *See* eBay, How Feedback Works, http://pages.ebay.com/help/feedback/howitworks.html (last visited Apr. 13, 2010).

comments.[138] These ratings contribute to users' numerical "Feedback Score," which eBay displays when those users sell or bid on items.[139] Clicking on an individual's user name or Feedback Score reveals text feedback that person has received.[140]

As discussed above, a good reputation assists sellers on eBay.[141] Many books and compact discs are available that provide advice on how to develop a positive reputation on eBay.[142] eBay is big business, with over $100 billion in sales of used goods in 2008.[143] These figures are striking since buyers must transact with total strangers who could easily swindle them;[144] yet, thanks in significant part to its reputation system, eBay succeeds.[145]

2. Wikipedia

On Wikipedia, the "free encyclopedia,"[146] anyone can edit most articles.[147] Most

[138] *See id.* Buyers can also leave more detailed numerical ratings for sellers, rating the sellers in response to four questions posed by eBay on a scale of one to five. *See* eBay, About Detailed Seller Ratings, http://pages.ebay.com/help/feedback/detailed-seller-ratings.html (last visited Apr. 15, 2010).

[139] *See* How Feedback Works, *supra* note 137.

[140] *See id.*

[141] *See supra* note 46 and accompanying text.

[142] *See* Amazon.com, http://amazon.com (a search in all departments for "how to sell on eBay," in quotation marks, reveals 66 books, DVDs, and similar products) (last visited Apr. 13, 2009).

[143] *See* eBay, 2008 Annual Report 1 (2008), *available at* http://investor.ebay.com/annuals.cfm (click 2008 Annual Report - Interactive Annual Report).

[144] *See* Fahri Unsal & G. Scott Erickson, *Online Auctions: A Review of Literature on Types of Fraud and Trust Building*, *in* Trust and New Technologies: Marketing and Management on the Internet and Mobile Media 40, at 91, 94–97 (Teemu Kautonen & Heikki Karjaluoto eds., 2008).

[145] *See id.* at 102–04 (describing how eBay's feedback system builds trust). In addition to its reputation system, eBay facilitates trust by insuring some transactions and maintaining a multi-step dispute resolution process. *See* Johnson, *supra* note 109, at 970 (describing how the dispute resolution system contributes to transaction success and customer satisfaction); Unsal & Erickson, *supra* note 144, at 97 (explaining how eBay insures some transactions).

[146] Wikipedia, http://wikipedia.org (last visited Apr. 15, 2010). The focus of this Article is the governance of the English-language Wikipedia.

[147] *See* Zittrain, *supra* note 2, at 133; Myers, *supra* note 78, at 167 & n.30.

changes are viewable instantaneously.[148] Individuals need not register to edit articles, though unregistered users' IP addresses are displayed in conjunction with their edits.[149] Despite the apparent potential for abuse, Wikipedia is a staggering success. There are over 3,200,000 articles in English, articles in 272 languages, and an estimated average 79 million unique monthly visitors from the United States as of April 2010.[150] A widely-publicized study found the accuracy of English language articles in Wikipedia equal to those in *Encyclopedia Britannica*.[151]

How is quality ensured when anyone can edit Wikipedia? The transparency of Wikipedia makes it easy to correct mistakes.[152] Each encyclopedia entry has a history page that displays a list of every change made and the user name (or IP address) of the author who made the change.[153] Entries can be reverted to any prior version easily.[154] Each entry also has an attached discussion page where editors can share ideas and debate what should be said.[155] Like articles, registered users each have pages that list all of the edits they have made and discussion pages where other editors can offer praise or criticism.[156] Additionally, automated programs clean up the work of the most obvious vandals.[157] To prevent libel, alterations to articles about living people by unregistered or inexperienced editors must be "flagged," or approved, by experienced editors before they

[148] *See* Zittrain, *supra* note 2, at 133; Wikipedia, Protection Policy, http://en.wikipedia.org/wiki/Wikipedia:Protection_policy (last visited Apr. 15, 2010) (describing limitations on who can edit certain articles).

[149] *See* Wikipedia, Why Create an Account?, http://en.wikipedia.org/wiki/Wikipedia:Why_create_an_account (last visited Apr. 15, 2010). Additionally, only registered users whose accounts have existed for at least four days and who have made at least ten contributions can edit "semi-protected" pages. *See id.*

[150] *See* Quantcast, Wikipedia.org, http://www.quantcast.com/wikipedia.org (last visited Apr. 4, 2010) (stating estimate of visitors); Wikimedia Meta, List of Wikipedias, http://meta.wikimedia.org/wiki/List_of_Wikipedias (last visited Apr. 4, 2010) (stating number of languages); Wikipedia, http://en.wikipedia.org (last visited Apr. 4, 2010) (stating number of articles in English).

[151] *See* Jim Giles, *Internet Encyclopedias Go Head to Head*, 438 Nature 900 (2005).

[152] *See* Zittrain, *supra* note 2, at 137.

[153] *See id.* at 133–34; Myers, *supra* note 78, at 167–68. The IP addresses of unregistered editors are displayed in place of user names. *See* Why Create an Account?, *supra* note 149.

[154] *See* Zittrain, *supra* note 2, at 133–34.

[155] *See id.* at 134.

[156] *See id.* at 136. Zittrain describes the practice of Wikipedians awarding each other "barnstars," digital images of stars that represent thanks for high-quality editing. *See id.*

[157] *See id.* at 137–138; Myers, *supra* note 78, at 168.

are publicly displayed.[158] Wikipedian leaders, called administrators, can ban the accounts or even IP addresses of especially abusive editors.[159]

Wikipedia's governance is not purely bottom-up. As already discussed, experienced editors have certain powers beyond those of new editors, and administrators have authority beyond other experienced editors.[160] To be promoted to administrator status, editors must apply to existing administrators and receive roughly 75% approval.[161] Wikipedia also has a handful of "bureaucrats" who are appointed by Wikipedia founder Jimbo Wales and possess authority above all other users.[162]

Despite some elements of an aristocracy at the tip of the iceberg, Wikipedians have developed a robust bottom-up culture.[163] Its editors have produced extensive guidelines for each other.[164] However, they also encourage experimentation; one of the guidelines is "be bold" in editing.[165] Though conflict arises thanks to this permissive attitude, Wikipedia has extensive dispute resolution systems.[166] The result of Wikipedia's openness is a strong community of regular editors, and Jonathan Zittrain highlights the site as a model of netizenship.[167]

[158] See Noam Cohen, *Wikipedia to Limit Changes to Articles on People*, N.Y. Times, Aug. 24, 2009, at B1, *available at* http://www.nytimes.com/2009/08/25/technology/internet/25wikipedia.html.

[159] *See* Zittrain, *supra* note 2, at 136.

[160] *See* Myers, *supra* note 78, at 169 (describing administrators' authority).

[161] *See id.*; Wikipedia, Guide to Requests for Adminship, http://en.wikipedia.org/wiki/Wikipedia:Guide_to_requests_for_adminship (last visited Apr. 15, 2010).

[162] *See* Zittrain, *supra* note 2, at 135–36, 138–41; Myers, *supra* note 78, at 169; Wikipedia, Bureaucrats, http://en.wikipedia.org/wiki/Wikipedia:Bureaucrats (last visited Apr. 15, 2010).

[163] Wikipedia's page describing administrators' roles begins with an emphatic statement that being one is "[n]o big deal." Wikipedia, Administrators, http://en.wikipedia.org/wiki/Wikipedia:Administrators (last visited Apr. 15, 2010).

[164] *See* Myers, *supra* note 78, at 169–70.

[165] Wikipedia, Be Bold, http://en.wikipedia.org/wiki/Wikipedia:Be_bold (last visited Apr. 15, 2010).

[166] *See generally* Wikipedia, Dispute Resolution, http://en.wikipedia.org/wiki/Wikipedia:Dispute_resolution (last visited Apr. 15, 2010).

[167] Zittrain, *supra* note 2, at 146–48.

3. Slashdot

Slashdot bills itself as conveying "news for nerds" about "stuff that matters," and its posts cover technology, science, software, gaming, and cyberlaw.[168] Slashdot maintains an innovative distributed moderation system for its comment section. Moderators are selected semi-randomly at preset intervals from regular commenters.[169] Moderators can rate users' comments on a series of pre-set characteristics, such as "insightful," "funny," or "troll," on a scale ranging from +5 (best) to -1 (worst).[170] Ratings are visible to readers alongside comments.[171] Comments with sufficiently positive ratings move up on the list of comments so visitors see them sooner, while comments with low ratings are invisible to readers who are not logged in.[172] Logged-in users can adjust their "thresholds" for low-rated comments so that more or fewer comments are displayed to them.[173] Over time, based on ratings received and other on-site actions, commenters develop "karma," a verbal grade on a scale ranging from "[t]errible" to "[e]xcellent."[174] Karma can affect the placement of all of an individual's comments as well as that person's ability to become a moderator.[175] To prevent abuses, a "meta-moderation" system also exists for rating moderators.[176]

4. Commonalities

There are several commonalities among these widely-praised sites. First, despite their large number of visitors, the sites provide easy methods for users to view each others' reputational information. Second, reputation development is reciprocal; those who wish to comment on others' behavior must also open themselves to being rated.

[168] Slashdot, http://slashdot.org (last visited Apr. 15, 2010). For an excellent summary of Slashdot's features, *see* Froomkin, *supra* note 136, at 863–67.

[169] *See* Slashdot, FAQ—Comments and Moderation, http://slashdot.org/faq/com-mod.shtml (last visited Apr. 15, 2010).

[170] *See id.*

[171] *See id.*

[172] *See id.*

[173] *See id.*

[174] *See* Slashdot, FAQ—Comments and Moderation, http://slashdot.org/faq/com-mod.shtml (last visited Apr. 15, 2010).

[175] *See id.*

[176] *See* Slashdot, FAQ – Meta-Moderation, http://slashdot.org/faq/metamod.shtml (last visited Apr. 15, 2010).

Third, the sites do not merely expect norms to emerge in a vacuum, but instead contain code designed to help foster social governance. Finally, they give users incentives to opt into the norm system and to take it seriously[177] As a result, they attract a high number of dedicated participants.

B. Failure of Norms: The Web as "Classic Counterexample"

While a handful of sites, like those described above, have had success with norm-driven user governance, most sites have failed to inculcate any sense of "netizenship" in visitors. This Sub-Part explores the reasons for that failure, which relate to the Web's structure.

First, the Web is too big and heterogeneous to be a unified community.[178] Second, the value of social capital on the Web is low since it cannot be transferred effectively between sites.[179] The low value of social capital hurts "netizenship" because the cost of norm creation is high.[180] Web users have insufficient incentives to invest themselves in individual Web communities, so the communities lack the critical mass of participation needed for norm generation.

Third, freedom of movement online undercuts our ability to police one another. In contrast to the offline world, people on the Web are not channeled into natural communities by geography.[181] While the Internet offers radically more freedom of choice in peer groups than is available offline, the decreased cost of site entry and exit renders social sanctions ineffective.[182] A participant in an online community need not suffer the indignity of the sanction since he or she may leave easily and join a similar community on a different site where the sanction cannot follow.[183] If a site does not engage in IP-address based blocking techniques, the sanctioned party can also return to

[177] For instance, on Wikipedia, users can edit without registering, but their changes are less likely to stay in the long-term. *See* Posting of Ed H. Chi to Augmented Social Cognition, Part 2: More Details of Changing Editor Resistance in Wikipedia, http://asc-parc.blogspot.com/2009/08/part-2-more-details-of-changing-editor.html (Aug. 7, 2009, 19:09 EST).

[178] *See* Lemley, *supra* note 110, at 1267–73. Lemley wrote almost a decade ago, and the Web has grown substantially since that time. *See supra* note 25.

[179] *See supra* Part II.B.

[180] *See* Netanel, *supra* note 65, at 432.

[181] *See* Johnson & Post, *supra* note 115, at 1370–76 (explaining how cyberspace undermines geographic boundaries).

[182] *See infra* Part VII.C.1–3.

[183] *See id.*

the same community under a different user name, unhindered by the sanction.[184] The combination of insufficient incentives for quality contributions and insufficient deterrence for low-quality contributions engenders the "flame-ridden cacophony" criticized by Neil Netanel.

Moreover, feelings of disinterest in the welfare of fellow users are exacerbated by the dehumanizing nature of Web communication. Robert Putnam, in his classic work on community association and politics, *Bowling Alone*, writes that trust and collaboration are in short supply on the Internet because "interaction is anonymous and not nested in a wider social context."[185] On the Web, we may see each other not as real people, but as just a few lines of text.[186] Although the introduction of broadband has offered more opportunities for multimedia presentations of self,[187] these still cannot convey the same sense of "personhood" as a brief in-person interaction. Additionally, without social intermediaries, I may see you only as a commenter on a political blog; I do not also see that you have a family, or are interested in jazz, or are a military veteran. It is thus easy for me to invest you with far less than full personhood. If I do not agree with you politically, I may be inclined to dismiss you as mistaken and worthless. Dehumanization increases abusive behavior, undermining social cohesion. As Danielle Citron explains, social psychology research indicates that it is much easier for people to victimize others who they do not invest with full humanity.[188] Individuals mediated by computers are more likely to victimize each other than those meeting face-to-face, even when using the Internet makes attackers no less likely to be caught.[189]

Given these and other factors, Neil Netanel described virtual communities on the Web as a "classic counterexample[]" to the type of situation in which norms would succeed in constraining individual behavior.[190] Although Netanel wrote almost a decade ago, his assertion has remained largely correct. Nevertheless, as the next Part describes, change is coming.

[184] *See* Citron, *supra* note 7, at 104.

[185] Putnam, *supra* note 37, at 176.

[186] *See* Citron, *supra* note 7, at 84 ("Online groups also perceive their victims as 'images' and thus feel free to do anything they want to them.").

[187] *See* Kang, *supra* note 16, at 1156, 58.

[188] *See* Citron, *supra* note 7, at 82–84 (collecting sources).

[189] *See* Auerbach, *supra* note 56, at 1643–44 ("[T]he anonymity with which children can often post messages or create websites empowers them to be more hurtful because they can launch their invective with little fear of reprisal . . . ."); Citron, *supra* note 7, at 83–84 n.171 and accompanying text; Lyrissa Barnett Lidsky & Thomas F. Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 Notre Dame L. Rev. 1537, 1575 & n.178 (2007).

[190] Netanel, *supra* note 65, at 429.

V. INTRODUCING SOCIAL INTERMEDIARIES

This Part introduces social intermediaries, which I contend will act as "social glue"[191] to bind together users on the Web. I first describe and explain social intermediaries. Next, I summarize features that many leading social intermediaries have in common. Finally, I explain why social intermediaries are likely to become widely used.

A. Social Intermediaries: Glue for the Social Web

Social intermediary service Pluck, in a perceptive White Paper, highlights the striking division between websites on which identity would be useful and those on which it is contained.[192] The latter type of site, which Pluck labels "social destinations,"[193] are more commonly called social networks. A typical social network allows users to write a personal profile, communicate with those other users, and share photographs and other media.[194] Popular social networks in the United States include Facebook, MySpace, and LinkedIn.[195] Social networks are repositories for online identity and reputation.[196] As Patricia Abril observes, "[f]or [social networking site] participants, a web page or online profile constitutes their identity in cyberspace."[197] Yet until recently, social networks have been gated communities of within-site activity.

Social intermediaries are the cross-Web successors to social networks. This Sub-Part first describes the software backbone for social intermediaries. It then describes the sites that will form the face of the Social Web. The purpose of this discussion is not to contend that the particular tools described below will become prominent. My goal is instead to introduce examples of the kinds of features one should expect to encounter on the Social Web.

[191] For use of the term "social glue," see*, e.g.*, Sunstein, *supra* note 99, at 97.

[192] *See* Pluck, *supra* note 5, at 1–3.

[193] *See id.*

[194] Abril, *supra* note 49, at 13.

[195] *See id.* Different social networking sites are popular in different parts of the world. *See* Wikipedia, Social Network Service, http://en.wikipedia.org/wiki/Social_network_service (last visited Apr. 15, 2010).

[196] *See* Abril, *supra* note 49, at 14–15; Tal Z. Zarsky, *Law and Online Social Networks: Mapping the Challenges and Promises of User-Generated Information Flows*, 18 Fordham Intell. Prop. Media & Ent. L.J. 741, 747 (2008).

[197] Abril, *supra* note 49, at 13.

1. The Backbone: OpenID and Related Software

Because individuals must typically create a new user name and password combination for each site they use, it is easy for people to become overloaded and forget their passwords or forget which name goes with which site.[198] OpenID, a shared authentication system, aims to change this situation. OpenID allows users to "sign in to thousands of websites without ever needing to create another username and password."[199] Through OpenID, one account can unlock many sites.

Sites that are willing to allow users to sign in via OpenID are called "relying parties" by the OpenID Foundation.[200] As of November 2009, over 50,000 sites were relying parties, with the number steadily increasing since OpenID's founding in 2005.[201] Relying parties include Web giants like AOL, Google, Microsoft, and Yahoo!.[202] As a result of its growth, tech entrepreneur site VentureBeat recently stated that OpenID "is beginning to show signs of going more mainstream on the [W]eb."[203]

It is easy for users to obtain an OpenID-enabled account. In fact, many people already have "OpenIDs" without realizing it. This is true because there is no single OpenID account format. Instead, OpenID is designed to facilitate sign-in using accounts from third-party sites that have chosen to be OpenID "providers."[204] Google, AOL, Yahoo!, MySpace, and Twitter are all OpenID providers.[205] To illustrate, users could visit MyKMart.com, an OpenID relying party, and then choose to sign in using their Google accounts.[206] Thus, users do not have to know that OpenID exists to enjoy its

[198] *See* Aresty, *supra* note 12, at 148–49.

[199] *See* OpenID, Benefits of OpenID, http://openid.net/get-an-openid/individuals (last visited Apr. 15, 2010).

[200] *See, e.g.*, OpenID Wiki, Relying Party Best Practices, http://wiki.openid.net/Relying-Party-Best-Practices (last visited Apr. 15, 2010).

[201] *See* OpenID, What is OpenID?, http://openid.net/get-an-openid/what-is-openid (last visited Apr. 15, 2010); Posting of Michael Olson to JanrRain Blog, Relying Party Stats as of July 1, 2009, http://blog.janrain.com/2009/07/relying-party-stats-as-of-july-1-2009.html (July 15, 2009, 16:40 EST); *see also* MyOpenID, OpenID Site Directory, https://www.myopenid.com/directory (last visited Apr. 15, 2010) (providing directory of OpenID relying parties).

[202] *See* OpenID Foundation Website, http://openid.net (last visited Apr. 15, 2010).

[203] Posting of Eric Eldon to VentureBeat, Single Sign-On Service OpenID Getting More Usage, http://digital.venturebeat.com/2009/04/14/single-sign-on-service-openid-getting-more-usage (Apr. 14, 2009).

[204] *See* OpenID, Get an OpenID, http://openid.net/get-an-openid (last visited Apr. 15, 2010).

[205] *See id.*

[206] *See* MyKmart, http://mykmart.com (click "log in") (last visited Apr. 15, 2010).

benefits.[207]

OpenID is open-source software.[208] Being open-source means that anyone can see OpenID's source code (human-readable programming code), anyone can edit OpenID's software, and anyone can install OpenID for free.[209] Brad Fitzpatrick, described as the father of OpenID, stated: "Nobody should own this. Nobody's planning on making any money from this. . . . It benefits the community as a whole if something like this exists, and we're all a part of the community."[210]

Security is the largest concern with regard to OpenID. OpenID contends that it is more secure than traditional password systems.[211] Specifically, OpenID asserts that because each individual's password is stored on only one provider's site, the chance of theft is decreased compared to using many passwords stored on multiple sites.[212] However, OpenID creates the risk of phishing, or theft of personal information through deception.[213] Specifically, malicious relying parties could use programming tricks to swipe users' passwords and then use those passwords to access the users' data on other OpenID-enabled sites.[214] The OpenID community recognizes that phishing is a risk and is working to develop technological and education-based solutions.[215]

OpenID is part of what Joseph Smarr labels the "Open Stack."[216] The Open Stack, according to Smarr, is a set of open-source technical standards designed to

[207] There exist, however, a number of standalone OpenID provider sites, which exist specifically to allow users to obtain OpenIDs. *See* Get an OpenID, *supra* note 204 (listing examples).

[208] *See* What is OpenID?, *supra* note 201.

[209] *See* OpenID, Developers, http://openid.net/developers (last visited Apr. 15, 2010) (inviting programmers to help develop OpenID); OpenID, Intellectual Property, http://openid.net/intellectual-property (last visited Apr. 15, 2010). *See generally* Benkler, *supra* note 106, at 63–67 (describing open-source software, as well as "free software," open source's more radical analogue).

[210] *See* Intellectual Property, *supra* note 209.

[211] *See* Benefits of OpenID, *supra* note 199.

[212] *See id.*

[213] *See* OpenID Wiki, OpenID Phishing Brainstorm, http://wiki.openid.net/OpenID_Phishing_Brainstorm (last visited Apr. 15, 2010); *see also* Wikipedia, OpenI—Security and Phishing, http://en.wikipedia.org/wiki/Openid#Security_and_phishing (last visited Apr. 15, 2010).

[214] *See* OpenID Phishing Brainstorm, *supra* note 213 (describing typical phishing attack).

[215] *See id.*

[216] Smarr, *supra* note 13.

facilitate the spread of social networking features.[217] Like OpenID, the remaining Open Stack features are designed to be invisible to typical users. Also like OpenID, other components of the Open Stack have grown in popularity quickly.[218]

One component of the Open Stack is OpenSocial, a package of application programming interfaces ("APIs") that allow programmers to design applets for social networks that support its standards.[219] In other words, OpenSocial provides a method for third-parties to add activities such as games, surveys, and personal organizers to social networking sites. Sites including LinkedIn, Friendster, and Google accept applets programmed on OpenSocial.[220] Facebook has a competing API for its network, called the "Graph API."[221]

Also included in the Open Stack is OAuth, the Web's "valet key."[222] Through OAuth, which complements OpenID's functions, users can allow one website limited access to their private data stored remotely on a different website.[223] OAuth powers Facebook Open Graph's cross-Web account authentication system.[224] PortableContacts, the fourth component of the Open Stack, is a newer project being spearheaded by Smarr and others to enable individuals to build a single, portable Web address book.[225]

OpenID and the Open Stack, or their competitors, will be the backbone of the emerging Social Web. Most notably as it relates to norms and reputation, OpenID and OAuth provide powerful tools for employing the same accounts across many websites. The next sub-Part will explore the user-facing social intermediary sites, which build upon the software foundations discussed above.

[217] *Id.*

[218] *See* Smarr, *supra* note 13.

[219] *See* OpenSocial, http://www.opensocial.org (last visited Apr. 15, 2010).

[220] *See id.*

[221] *See* Facebook, Graph API, http://developers.facebook.com/docs/api (last visited May 5, 2010).

[222] *See* Eran Hammer-Lahav, OAuth, Introduction, Sept. 5, 2007, http://oauth.net/about.

[223] *See id.*

[224] *See* Facebook, Authentication, http://developers.facebook.com/docs/authentication/ (last visited May 5, 2010).

[225] *See* Portable Contacts, http://portablecontacts.net (last visited Apr. 15, 2010). The final component of the Open Stack, XRD 1.0, is a technical protocol for data retrieval. *See* Smarr, *supra* note 13; Wikipedia, XRDS, http://en.wikipedia.org/wiki/XRDS (last visited Apr. 15, 2010).

2. The Face of the Social Web

The tools described in this Sub-Part represent examples of the intermediaries through which users seeking cross-Web functionality will interact. These tools channel the programming frameworks described above into specific features for site operators and users. I refer to these tools as social intermediaries since they are the cross-Web evolution of social networks.[226]

Presently, the two most ambitious social intermediary projects are Google Friend Connect and Facebook's Open Graph. Perhaps not coincidentally, both Google Friend Connect and Open Graph's predecessor, Facebook Connect, were first made public in preliminary "beta" form on December 4, 2008.[227] As of December 2009, over 60,000 websites had already adopted Facebook Connect (similar statistics are not readily available for Google Friend Connect).[228]

Google Friend Connect promises site operators that it can help them build communities without requiring complex programming.[229] First, site operators can choose from a catalog of applets programmed on the OpenSocial API.[230] For instance, Friend Connect offers applets that allow visitors to leave comments, rate and review site content, become site "members," and advertise content to others.[231] Building on the Open Stack framework, Friend Connect also gives users options for choosing their account providers. Users can interconnect their on-site actions to their existing Google accounts, including their Google profiles and Gmail addresses.[232] Alternatively, users can represent

[226] As Smarr notes, site operators who are skilled programmers may prefer to build social features directly from the Open Stack (or its proprietary competitors) rather than using the easy-to-deploy systems described in this Sub-Part. *See* Smarr, *supra* note 5. For simplicity, I will refer to all implementations of Social Web features as using social intermediaries.

[227] *See* The Official Google Blog, Google Friend Connect: Now Available, http://googleblog.blogspot.com/2008/12/google-friend-connect-now-available.html (Dec. 4, 2008, 11:48 EST); Posting of Mark Zuckerberg to The Facebook Blog, Facebook Across the Web, http://blog.facebook.com/blog.php?post=41735647130 (Dec. 4, 2008, 12:18 EST).

[228] *See* Don Reisinger, *A Year On, Facebook Connect Shows Fast Growth*, CNET News, Dec. 10, 2009, http://news.cnet.com/8301-17939_109-10412985-2.html.

[229] *See* Google Friend Connect, http://www.google.com/friendconnect (last visited Apr. 15, 2010).

[230] *See id.*; Google Social Web Blog, Introducing the Google Friend Connect API, http://googlesocialweb.blogspot.com/2009/03/introducing-google-friend-connect-api.html (Mar. 12, 2009, 8:22 EST).

[231] *See* Google Friend Connect, Gadget Gallery, http://www.google.com/friendconnect/home/gadgets?hl=en (last visited Apr. 15, 2010).

[232] *See* Posting of Mark O'Neill to makeuseof.com, Get Your Google Profile Organized for Friend Connect, http://www.makeuseof.com/tag/get-your-google-profile-organized-for-friend-connect (Dec. 8, 2008). Google profiles allow Google users to list details about themselves. *See*

themselves with accounts from OpenID providers other than Google and can incorporate personal information stored on third-party providers' sites into Friend Connect-enabled sites.[233]

Facebook's Open Graph advertises a similar array of features,[234] but with special emphasis on integrating with the existing Facebook social network. For instance, when users visit a Facebook-enabled site, they can see what content on that site has been popular with their Facebook "friends" and choose to share content they enjoy with others.[235] One key feature of Open Graph is that sites can add a "like" or "recommend" button; when users click the button, it adds a link to the site on their Facebook profiles, shares the link with their Facebook friends, and displays their names and photographs to Facebook friends who visit.[236] When users participate on a site via Open Graph, Facebook promises the site operator access to data including the user's name, photograph, and Facebook friends.[237] It also promises operators the ability to integrate their content with Facebook, such as by adding items to users' "story streams" and by communicating to users' friends via Facebook notifications.[238]

Open Graph is distinct in light of Facebook's unique emphasis on "real life," offline identity. Facebook's terms of service state that "Facebook users provide their real names and information," and they prohibit users from providing any false personal information.[239] Facebook's terms also permit only one account per individual.[240] Facebook also has engaged in an active campaign of deleting clearly fake profiles, resulting in the mistaken deletion of legitimate accounts.[241] Leading competitors typically do not prevent users from adopting pseudonyms or creating multiple

Google, Create Your Profile, http://www.google.com/profiles (last visited Apr. 15, 2010). Gmail is Google's Web-based email service. *See* Gmail: Email from Google, http://mail.google.com (last visited Apr. 15, 2010).

[233] *See* Google Friend Connect, Awaken and Strengthen Your Community,. http://www.google.com/friendconnect/home/overview?hl=en (last visited Apr. 15, 2010).

[234] *See* Facebook, *supra* note 17.

[235] *See id.*

[236] *See* Facebook, Like Button, http://developers.facebook.com/docs/reference/plugins/like (last visited May 5, 2010); Iskold, *supra* note 16.

[237] *See* Facebook, *supra* note 17.

[238] *See id.*

[239] *See* Facebook, Statement of Rights and Responsibilities, § 4, Apr. 22, 2010, http://www.facebook.com/terms.php.

[240] *See id.* § 4(2).

[241] *See* Grimmelmann, *supra* note 12, at 1198; Barbara Ortutay, *Got an Unusual Name? Facebook May Think It's Fake*, ABC News, May 18, 2009, http://abcnews.go.com/Technology/AheadoftheCurve/wireStory?id=7614876.

accounts.[242]

Facebook and Google Friend Connect seek to offer features applicable to all websites. More narrowly, a number of companies, including Disqus, JS-Kit, IntenseDebate, Pluck, and KickApps, all offer tools focusing on commenting systems for blogs and other similar sites.[243] All five of the companies mentioned above allow users to leave comments on multiple supporting blogs with the same account.[244] They also permit users to create central profiles in which they can input personal information.[245] On all five, profiles also act as easily accessible records of all commenting activities for each user.[246] Additionally, these social intermediaries have "friending" features; for instance, on Disqus, individuals can choose to "subscribe" to commenters they like so that they can see all of their future comments.[247] They also offer powerful tools for site moderation.[248] All five support login via many OpenID providers as well as via Facebook.[249] In addition, JS-Kit allows users to sign into its system using multiple accounts simultaneously, so that they can share their activities through multiple social networks simultaneously.[250]

The reputation and rating systems of Disqus and IntenseDebate are especially notable. Disqus and IntenseDebate allow users to choose whether to rate comments positively or negatively.[251] Users must be logged in to their own accounts to rate others'

[242] *See, e.g.*, Google Terms of Service, April 16, 2007, http://www.google.com/accounts/TOS; Myspace.com Terms of User Agreement, June 25, 2009, http://www.myspace.com (click "terms").

[243] *See* JS-Kit Community Wiki, Feature-List, Aug. 28, 2009, http://wiki.js-kit.com/Feature-List.2009-08-28-16-35-36 (comparing features of competitors). *See generally* Disqus Comments, http://www.disqus.com (last visited Apr. 15, 2010); IntenseDebate: Imagine Better Comments, http://www.intensedebate.com (last visited Apr. 15, 2010); JS-Kit ECHO, http://js-kit.com (last visited Apr. 15, 2010); KickApps, http://www.kickapps.com (last visited Apr. 15, 2010); Pluck: Integrated Social Media Solutions for Leading Digital Destinations, http://pluck.com (last visited Apr. 15, 2010).

[244] *See* Feature-List, *supra* note 243.

[245] *See id.*

[246] *See id.*

[247] *See, e.g.*, Disqus Profile, Your Comments, Your Control, http://www.disqus.com/profile (last visited Apr. 15, 2010).

[248] *See* Feature-List, *supra* note 243.

[249] *See id.*

[250] *See id.* Plaxo also has a system for taking data from multiple social networks. S*ee* Grimmelmann, *supra* note 12, at 1193–94 (describing Plaxo's "screen-scraper" tool).

[251] *See* Disqus, Help, http://help.disqus.com/ (last visited Apr. 15, 2010); IntenseDebate,

comments.[252] As participants comment more and receive more ratings, they obtain "clout points" (on Disqus) or "reputation points" (on IntenseDebate), which are calculated according to undisclosed algorithms.[253] These ratings are then displayed along with users' comments.[254] To protect the quality of its rating system, Disqus allows only experienced users to rate others, and it forbids self-serving and collusive ratings.[255] Disqus also intends to allow site operators to moderate based on clout points.[256]

Site operators are not presently limited to using only one of the above-described systems. Social intermediary services including Facebook and Google allow sites to implement features from multiple providers.[257] It is not uncommon for sites to give users a choice of identity providers and to offer social features from a number of services.[258]

While the systems described above are focused on exporting social features to outside sites, companies such as Google are bringing blog consumers to enclosed ecosystems containing social features. Through Google Reader, people can subscribe to all of the blogs and other syndicated websites they enjoy and read them together in one place.[259] Recently, Google has been introducing social features to Google Reader. Users can choose to "share" blog posts they enjoy with others who also use Google Reader and to "follow" those whose shared posts they wish to read.[260] Users can also offer comments on articles within Google Reader without posting on the actual blog's

Features, http://www.intensedebate.com/features (last visited Apr. 15, 2010).

[252] *See* Help, *supra* note 251; IntenseDebate: Imagine Better Comments, *supra* note 243 (click "users" tab).

[253] *See* Help, *supra* note 251; Features, *supra* note 251.

[254] *See* Help, *supra* note 251; Features, *supra* note 251.

[255] *See* Help, *supra* note 251.

[256] *See id.*

[257] *See* Posting of Mike Kirkwood on ReadWrite Cloud, Bringing Google, Facebook, Twitter Together: Third-Party Login Grows Rapidly in 2010, http://www.readwriteweb.com/cloud/2010/04/trends-peer-pressure-is-all-th.php (Apr. 26, 2010, 23:10 EST).

[258] Companies such as JanRain facilitate the implementation of social features from multiple social intermediaries by providing technical implementation skills to site operators. *See* JanRain, http://www.janrain.com (last visited May 5, 2010).

[259] Many blogs and other websites syndicate their content in formats like RSS or Atom, which allow users to "subscribe" to their content through programs such as Google Reader. *See* Wikipedia, Web Syndication, http://en.wikipedia.org/wiki/Web_syndication (last visited Apr. 15, 2010).

[260] *See* Google, Reader Help, Sharing With Friends, http://www.google.com/support/reader/bin/answer.py?hl=en&answer=83000 (last visited Apr. 15, 2010).

comment section.[261] Individuals can also mark that they "like" an article; the names of all the users who "liked" an article then appear at the top of that article for everyone who views it through Google Reader.[262]

B. Summary of Features of Social Intermediaries

While the social intermediaries described above vary, and new competitors may emerge, certain features are common to multiple providers. For convenience, this Sub-Part will summarize some of the common features to which the remainder of this Article will refer regularly.

Site operators who install social intermediaries will gain the ability to add social features to their site. They will also gain the ability to moderate user activity with greater ease and greater strength. On most social intermediaries, each user will have:

- The ability to add content to third-party websites under a consistent account
- A "friending" or "following" ability, by which users can gain easier or greater access to the profiles of, and other information concerning, a select subset of fellow users
- Privacy controls analogous to those on social networks, by which users can choose to restrict the public availability of the information described above
- A profile page that is easily accessible from third-party sites on which the user has participated via the social intermediary. The profile page may contain the following features:
  - Areas for the user to describe himself or herself
  - Space for images or other multimedia content, including pictures of the user
  - Automatically compiled information linking to all of the user's cross-Web activity employing the social intermediary
  - A section in which other users can comment publicly to the user
  - A list of all of the "friends" or "followers" of the user, along with links to their profiles

While only available at this time on a minority of social intermediaries, the "reputation score" systems used by Disqus and IntenseDebate also are of particular importance for the remainder of this Article.

[261] *See* Google, Reader Help, About Comments, http://www.google.com/support/reader/bin/answer.py?hl=en&answer=142213 (last visited Apr. 15, 2010).

[262] *See* Google, Reader Help, Using the Like Button, http://www.google.com/support/reader/bin/answer.py?hl=en&answer=154622 (last visited Apr. 15, 2010).

C. Likelihood of Popularity

It is easy to make mistaken predictions about the importance of a hypothesized technological and social trend that fails to materialize.[263] Before analyzing the impact of the Social Web on norms and law, it is important to determine whether there will *be* a Social Web. Accordingly, this Sub-Part will suggest why social intermediaries are likely to grow in popularity with both site operators and end users.

1. Advantages for Site Operators

Site operators have much to gain from social intermediaries. Most importantly, social intermediaries allow them to incorporate user-generated content easily without requiring a high degree of programming skill. Social intermediaries are highly customizable; unlike the rigid and basic comment systems of the past, site operators are able to incorporate multimedia third-party content easily and flexibly. Moreover, social intermediaries make it far easier to regulate and moderate user behavior, enabling site operators to provide better user experiences and consistently high-quality content.[264]

Social intermediaries offer other benefits to site operators as well. Shared authentication makes it easier for users to begin participating on sites quickly.[265] Instead of spending time creating a new account information, visitors can begin engaging with a site's features immediately. Social intermediaries also provide capacity for "distributed advertising" to site operators.[266] Distributed advertising relies on users to spread information about sites or products they like to their acquaintances.[267] Distributed advertising may be more valuable than conventional advertising because it is free,

[263] *See* Putnam, *supra* note 37, at 166–70 ("The early, deeply flawed conjectures about the social implications of the telephone warn us that our own equally early conjectures about the Internet are likely to be similarly flawed.").

[264] *See infra* Part VII.B.2 (describing how site operators can moderate using social intermediaries).

[265] *See* OpenID, Add OpenID to Your Site, http://openid.net/add-openid (last visited Apr. 15, 2010); Pluck, *supra* note 5, at 7. Facebook reported a 30–200% increase in registration for sites using Facebook Connect, as well as a 15–100% increase in creation of user-generated content. *See* Pluck, *supra* note 5, at 7.

[266] *See, e.g.*, Disqus Comments, Powering Discussion on the Web, http://www.disqus.com/comments (click "This is why you should too...") (last visited Apr. 15, 2010).

[267] *See* Cecilia Zeniti, Note, *The Optimal Liability System for Online Service Providers: How Zeran v. America Online Got It Right and Web 2.0 Proves It*, 23 Berkeley Tech. L.J. 583, 613–14 (2008). *See generally* McGeveran, *supra* note 12 (describing the structure of social marketing).

acquaintances naturally share affinities, and people typically put more weight on their friends' recommendations over those of paid endorsers.[268] Facebook advertises that it gives sites access to the data in the personal profiles of users who have not opted out of "instant personalization."[269] Finally, since social intermediaries track users' cross-Web activities, they can give site operators access to useful marketing data about users.[270] Of course, as beneficial as distributed advertising, access to user data, and tracking features may be for site operators and advertisers, they raise serious privacy concerns for users.[271]

Not all site operators will want to install social intermediaries. Some might be content with static sites and uninterested in user-generated content. Operators of especially popular Web 2.0 sites, such as eBay, might already have well-developed communities and interface features and thus will see little to gain from social intermediaries.[272] Nevertheless, for many sites, social intermediaries appear likely to be attractive.

2. Advantages for Users

Many of the reasons social intermediaries will be attractive to consumers overlap with the reasons for their value to site operators. First, shared authentication makes it easier for first-time visitors to access a new site's features. Second, distributed advertising can make it easier for consumers to find sites they will enjoy. Third, social intermediaries introduce new opportunities for building online social circles; users can make new acquaintances on one site they visit and then can interact with them across the Web. Most importantly, users can begin to compile reputational data from their activities across the Web.[273]

The leading drawback of social intermediaries for users is loss of privacy.[274] There is some evidence of a privacy-based backlash against Facebook's especially aggressive implementation of its social intermediary software.[275] Nevertheless, in

[268] *See* Zeniti, *supra* note 267, at 613–14.

[269] *See* Facebook, *supra* note 17.

[270] *See, e.g.*, *id.* (describing benefits of its "Insights" analytics system).

[271] *See* McGeveran, *supra* note 12 (discussing privacy implications of social marketing); Schumer et al., *supra* note 19 (expressing concern with Facebook's data retention).

[272] *Cf.* Picker, *supra* note 8, at 6–7 (expressing concern that sites like eBay would act to prevent reputation portability).

[273] *See infra* Part VI.B.

[274] *See* Grimmelmann, *supra* note 12, at 1148 n.53; McGeveran, *supra* note 12, at 1161–62.

[275] *See* Posting of Mike Melanson to ReadWriteWeb, The Facebook Backlash Has Begun . . .

general, privacy-ceding electronic media applications such as existing social networks and location-based games have only grown in popularity,[276] particularly among young people.[277] This implies that many users are willing to trade privacy for connectivity. In *Saving Facebook*, however, James Grimmelmann suggests that cognitive biases prevent people from sufficiently appreciating the privacy risks of social networking sites.[278] If he is correct, similar errors in judgment may be at play in users' decisions to participate on sites that employ social intermediaries. Facebook's opt-out approach and ever-changing privacy policy may especially obfuscate privacy risks for users.[279] Nevertheless, regardless of whether the trend towards interconnection is based on conscious choice or instead based on lack of understanding, it is reasonable to expect this trend to continue, so that social intermediaries' popularity will grow notwithstanding privacy concerns.

E. Network Effects

There is an additional reason to believe social intermediaries might become widely used. Based on "network effects," if one or a few social intermediaries become popular, their value will increase, leading to a potential upward cycle of adoption. In economic theory, the value of most goods does not vary with the number of people who possess and use them. My banana does not taste better if many other people are eating bananas simultaneously. In contrast, "network effects" apply to goods whose value increases as more people possess and use them.[280] Telephones are "network goods"; a

http://www.readwriteweb.com/archives/before_you_go_blocking_facebooks_instant_personali.php (Apr. 23, 2010, 7:25 EST) (noting informal evidence of backlash soon after Open Graph's debut); Posting of Robert Quigley to Geekosystem, Did the Great Facebook Deactivation Wave of 2010 Just Kick Off?, http://www.geekosystem.com/facebook-deactivate-wave (May 6, 2010, 14:15 EST) (describing announcement by two prominent technology writers that they eliminated their Facebook accounts, and noting that Google searches for the phrase "deactivate Facebook" have tripled since Open Graph's debut).

[276] *See, e.g.*, Facebook, Statistics, http://www.facebook.com/press/info.php?statistics (last visited Apr. 15, 2010) (stating Facebook has over 300 million active users); Wikipedia, Location-Based Game, http://en.wikipedia.org/wiki/Location-based_game (last visited Apr. 15, 2010) (listing electronic games in which success is based on position, as tracked by GPS).

[277] *See* John Palfrey & Urs Gasser, Born Digital: Understanding the First Generation of Digital Natives 22–37 (2008).

[278] *See* Grimmelmann, *supra* note 12, at 1160–64.

[279] *See* Posting of Pete Cashmore to Mashable, Nobody Can Stop Facebook Because Nobody Understands Facebook, Mashable, http://mashable.com/2010/05/04/facebook-privacy-report (Apr. 27, 2010); *see also* Posting of Kurt Opsahl to Electronic Frontier Foundation, Facebook's Eroding Privacy Policy: A Timeline, http://www.eff.org/deeplinks/2010/04/facebook-timeline (Apr. 28, 2010) (documenting changes to Facebook's privacy policy over time).

[280] *See generally* Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 Calif. L. Rev. 479 (1998).

telephone is useful only as a paperweight if nobody else has one.[281] Telephones are examples of "true" network goods, in that their "value lies in facilitating interactions between a consumer and others who own the product."[282]

Like telephones, social intermediaries are true network goods.[283] If a social intermediary gains a foothold among site operators and users, its value will increase, potentially leading to greater adoption. An upward spiral can result. Networked goods tend towards convergence on a single standard.[284] Social intermediary providers' awareness of this fact helps explain their rush to develop, deploy, and market these tools.[285] The possibility of capturing a significant portion of the market helps explain why Google and Facebook, which already have large bases of participants, have been at the forefront of developing social intermediaries. While convergence may occur in the future, at present competition is hot, and new competitors may emerge beyond those described above.

VI. Identity, Reputation and the Social Web

This Part will first show that social intermediaries enable individuals to project a consistent identity across much of the Web. It will then explain how social intermediaries open the reputation economy to everyone. It will then consider legal rules needed to protect the information value of portable reputational data. Finally, it will examine how social intermediaries humanize interactions on the Web, promoting a culture of respect for other people and other ideas.

A. Portable Identity Enabled

Social intermediaries bind together our previously disaggregated identities on the Web. I no longer must let others guess whether I am the same person from site to site based on *ad hoc* clues I might leave. As long as I sign in using the same account from the same OpenID provider (or competing account system), I show that my actions across multiple websites originate from the same source. Conversely, others cannot claim my social intermediary-facilitated activity as their own. Social intermediaries therefore remove much of the veil from agency on the Web.[286]

[281] *See id.* at 488.

[282] *Id.* at 491.

[283] *Id.* at 491.

[284] *See id.* at 496–97.

[285] *See generally id.* at 495 (noting that first-movers gain substantial advantages in competitions to market networked goods).

[286] Of course, even with social intermediaries, it is too much to say that consumers will

Of course, not all sites will accept accounts from the same providers. Accordingly, social intermediaries do not make it possible to maintain a single universal Web identity. Nevertheless, given the network effects-based advantages, it is reasonable to project that many sites will choose to accept accounts from popular providers. Therefore, it is likely that significant cross-site identity transfer will be possible.

In sum, social intermediaries go a great distance toward remedying the absence of identity information in the Internet's design. Rather than being located in the infrastructure layers, the ability to project a consistent identity across the Web is instead made available at the application layer.

B. Reputation Economy for Everyone

By making it easier for users to compile far richer reputational data, social intermediaries allow everyone to participate in the reputation economy. Rather than having their reputational information stranded on dozens of sites, users can build a single multi-site profile. Profiles can thus reflect an individual's diverse interests. Each user's profile can compile all of his or her cross-Web activity under that account. These compendiums of cross-Web activity scale easily; even if users participate thousands of times on hundreds of sites, the automated links generated can still be displayed and understood easily. Profiles can also provide information about online relationships built across many different sites. In each user's profile, his or her cross-Web "friends" can provide public messages, share links, and offer other information.

Users can only develop rich compilations of reputational information if they choose to act with the same accounts regularly. Except for Facebook, social intermediaries typically permit individuals to create multiple accounts.[287] Nevertheless, despite the privacy risks, it is reasonable to project that many users will employ the same accounts repeatedly.[288] First, signing in with the same account repeatedly saves time. More importantly, the incentives offered by the reputation economy will encourage individuals to use the same accounts across many sites.[289] Developing an account with strong reputational information will necessarily take time and effort. But other users' knowledge of the time and effort involved will itself signify an individual's quality.

Offline, naturally-occurring transaction costs prevent us from knowing reputational information about the vast majority of people. On the Social Web, it is easy to obtain rich information about any individuals who wish to let us know about

know with certainty that I am the same person from site to site. More than one individual might share a single account, or an account might be stolen. Still, with social intermediaries, we take an enormous step towards the possibility of unified cross-Web identity.

[287] *See supra* notes 239–42 and accompanying text.

[288] *But cf. infra* Part VII.C (describing how malicious users who intend to behave disruptively typically choose to act under "single-shot" accounts in order to escape sanction).

[289] Reputation economy incentives also likely will encourage many users to make their reputational information public, notwithstanding privacy risks.

themselves. Mass participation in the reputation economy will be promoted by a combination of ease of access to reputational data, the larger quantity of such data, and the increased certainty about whom that data concerns. In sum, while the reputation economy previously was generally available to celebrities such as Stephen Colbert and the Chris Anderson, "reputation riches" are now open to everyone.[290]

The result is a more efficient Web.[291] Without social intermediaries, social capital was locked, wastefully, in individual websites. Social intermediaries provide central banks for social capital and create the infrastructure necessary to allow users to transport reputation across sites.[292] Therefore, the value of reputation development will rise. More users will be motivated to leave better comments, sell more honestly, and create new works.

Just as social intermediaries benefit producers of goods and content on the Web, they also benefit consumers. Purchasers of goods will be better able to tell whether they are buying from an honest seller or a swindler. Similarly, content consumers will be better able to find material across the Web from creators whose work they enjoy. Moreover, social intermediaries make possible more frequent contextualization of information based on producer reputational data. For example, legitimate online grassroots organizers can demonstrate that they are not "astroturfers" since social intermediaries can reveal their long histories of activism for the cause in question.

C. Legally Protecting Social Intermediaries' Information Value

There is the possibility that social intermediaries' identity and reputational data systems could be manipulated, undermining their efficiency-creating informational value.[293] While social intermediaries clear up much of the uncertainty over whose online activity is whose, they still allow people to lie about their offline characteristics. Individuals might misrepresent their experience, expertise, or personal histories in order to promote their own interests. For instance, highly-regarded Wikipedia editor "essjay" bolstered his credentials on the site by falsely claiming to be a tenured university professor holding two doctorates.[294]

Beth Noveck writes that while traditional conceptions of identity would imply that online identity either "belongs" to the individual user or to the company that makes

[290] *See* Smarr, *supra* note 5 (suggesting the Social Web opens the benefits of social networking to the "long tail" of sites and users).

[291] *See* Smarr, *supra* note 13 (describing the Open Stack as a "classic case of removing inefficiency from the system").

[292] *Cf.* Pluck, *supra* note 5, at 1–3 (analogizing social intermediaries to bridges).

[293] *See generally* Palfrey & Gasser, *supra* note 277, at 17–22 (describing how with time and improved technology, creating new personas has become increasingly easy).

[294] *See* Wikipedia, Essjay Controversy, http://en.wikipedia.org/wiki/Essjay (last visited Apr. 15, 2010).

the identity available to others, these conceptions ignore the value of the identity to the community.[295] She argues that trademark law, which reflects the informational value of marks to third parties, should inform our understanding of how to regulate online identity.[296] We should build on Noveck's conceptual framework to develop flexible protections that take into account all parties' interests.

To allow users to take advantage of social intermediaries' expansion of the value of reputation, the law should act to limit deceptive self-identification that is socially harmful. In preventing wrongfully misleading self-identification, regulators should avoid prohibiting socially beneficial behavior. This is a fine line, requiring careful balancing. Individuals should be free to maintain fanciful identities on social intermediaries if they so choose, [297] even though this can enable abusive behavior.[298] Fanciful identities should also be encouraged, not prohibited. Online, "[w]e can . . . create vivid, visual representations of personal identity . . . independent of our offline attributes."[299] For many users who wish to explore identity beyond the limits necessitated by the offline world, the availability of multiple accounts is the "feature[,] not the bug[,]" of online socializing.[300] In some non-commercial circumstances, even intentional deceptions about offline identity may have social value and should not be prohibited.[301] Therefore, regulators should focus on limiting deceptive self-identification for commercial gain.

[295] *See* Beth Simone Noveck, *Trademark Law and the Social Construction of Trust: Creating the Legal Framework for Online Identity*, 83 Wash. U. L. Q. 1733, 1738–40 (2005); *see also* Solove, *supra* note 21, at 33–34 (noting that reputation is socially created); Susan P. Crawford, *Who's In Charge of Whom I Am? Identity and Law Online*, 49 N.Y.L. Sch. L. Rev 211, 213–15 (2005) (recognizing that "identity is a group project").

[296] *See* Noveck, *supra* note 295, at 1771–79.

[297] Legal restrictions on anonymity on social intermediaries would raise serious First Amendment issues. *See generally McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341-42 (1995) ("[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment."). In an analogous context, many courts require heightened showings before plaintiffs can enforce subpoenas that would unmask anonymous online speakers. *See, e.g., Solers, Inc. v. Doe*, 977 A.2d 941, 954-57 (D.C. 2009); *Indep. Newspapers, Inc. v. Brodie*, 966 A.2d 432, 457 (Md. 2009); *Doe v. Cahill*, 884 A.2d 451, 460-61 (Del. 2005); *Dendrite Int'l, Inc. v. Doe No. 3*, 775 A.2d 756, 760-61 (N.J. Super. Ct. App. Div. 2001).

[298] *See infra* Part VII.C (discussing "reputation reset").

[299] Noveck, *supra* note 295, at 1737.

[300] *Id.* at 1747–48; *see also* Crawford, *supra* note 295, at 215 (2005) (suggesting that online identity that is "unbundled" from offline identity "may be a concept whose time has now come").

[301] *See, e.g.*, Kang, *supra* note 16, at 1136–37, 1179–86 (describing "transmutation," a strategy by which a person pretends online to be of a different ethnicity or gender, thereby experiencing the social treatment of a person of those characteristics); *infra* notes 385–386 and accompanying text (discussing "transmutation" further).

Prohibiting commercial deception strikes an appropriate balance by focusing on the area in which deceptive behavior is most likely to be harmful to consumers without threatening areas in which free expression is most important. It also falls within the law's long-established role in consumer protection.[302]

Sale of social intermediary accounts should also be prohibited. Players of online multi-player games sell "powerful" characters and other items to each other.[303] In the gaming context, arguably, these transactions are harmless to third-party gamers since the purchasers are merely saving themselves time required to acquire enjoyable characters and items. In contrast, sales of social intermediary accounts harm the public since they undercut the signaling function of reputation development.[304] While social intermediary providers may prohibit account transfers through contract,[305] outright prohibition of account sale can add government enforcement capabilities and fully account for the interests of third parties.

Regulators must also protect social identities' informational value from social intermediary providers themselves. Providers may be tempted to assert absolute ownership over users' identities based on "clickwrap" agreements with users, regardless of the interests of users or third parties.[306] Therefore, the law should also discourage arbitrary decisions by social intermediary providers to terminate individuals' accounts, especially when individuals have invested time and effort into building their reputational data.[307] Absolute ownership claims by social intermediaries over user data can also threaten privacy.[308] However, the law also should not impose such rigid requirements on

[302] For instance, the Federal Trade Commission Act of 1914 prohibits "unfair or deceptive acts or practices in or affecting commerce," and most states have statutory prohibitions against seller misrepresentations. 15 U.S.C. § 45 (2006); *see* Mary Dee Pridgen, Consumer Protection and the Law § 2:1 (2008), *available at* West Database "CONPROT." The FTC recently has taken a more active role in regulating the Internet, requiring online writers to disclose when they are being paid to endorse products and services. *See* Guidelines Concerning the Use of Endorsements and Testimonials in Advertising, 74 Fed. Reg. 53,124 (Oct. 15, 2009) (to be codified at 16 C.F.R. §§ 255.0–255.5).

[303] *See* Noveck, *supra* note 295, at 1734–35 (describing story of one avatar auctioneer); Michael H. Passman, *Transactions of Virtual Items in Virtual Worlds*, 18 Alb. L.J. Sci. & Tech. 259, 261–63 (2009).

[304] *See* Unsal & Erickson, *supra* note 144, at 104 (describing how a growing market for false seller ratings on eBay could undermine the value of its feedback system).

[305] For instance, Facebook's terms of service prohibit transfer of accounts without written permission from Facebook. *See* Statement of Rights and Responsibilities § 4(7), *supra* note 239.

[306] *See* Crawford, *supra* note 295, at 212, 219–21 (noting online multi-player gaming companies' assertion of ownership over users' accounts); Noveck, *supra* note 295, at 1779.

[307] *See* Grimmelmann, *supra* note 12, at 1198 (criticizing Facebook for arbitrarily deleting accounts and suggesting it should adopt a due process model).

[308] Grimmelmann argues that data ownership rights are not sufficient to protect privacy.

social intermediary providers that they cannot efficiently develop and regulate their systems.[309]

D. Values Forwarded by Social Intermediaries: Culture of Respect and Access to Diversity of Ideas

While computer-mediated communication can dehumanize its participants by isolating their identities into bits and pieces,[310] social intermediaries introduce some positive steps towards full representation of personhood. Previously, on any given website, I may have appeared to be nothing more than some text or an image, and only my actions on that site were reflected. In contrast, my social intermediary profile can reflect my cross-Web activity, my personal profile information, and my social connections. My Web self begins to look more like a multi-dimensional person, with a variety of ideas, interests, and relationships.

Since dehumanization facilitates abusive behavior, the rounded expressions of personhood offered by social intermediaries may mitigate attacks. A potential troll might realize he or she has something meaningful in common with a potential victim and decide not to attack. Even if they have nothing in common, the potential attacker might still see in the possible victim a complete person who is worthy of respect.[311] Conversely, when someone *is* victimized on the Web, social intermediaries can facilitate the spread of information on the victim's plight. As more people learn of the harm caused by anonymous attacks online, potential trolls may come to understand the harms that can flow from such behavior and be dissuaded.

Social intermediaries also can help overcome self-segregation online. Cass Sunstein and others have expressed concern about the "echo chamber" effect of the Internet.[312] According to this view, individuals will only visit sites with which they are predisposed to agree and over time become radicalized.[313] Social intermediaries can

See id. at 1192–95. However, full social intermediary ownership of personal data is surely inimical to meaningful privacy controls for users.

[309] *Cf.* Zittrain, *supra* note 99, at 1978, 1995–96 (contending that rigid adherence to end-to-end principles would undermine ISPs' abilities to perform needed network maintenance).

[310] *See supra* Part IV.C.

[311] Social scientists have found, for instance, that racism can be diminished though interpersonal associations "of a sort that reveal[] enough detail about the member of the disliked group to encourage seeing him or her as an individual rather than as a person with stereotyped group characteristics." Norman Miller & Marilynn B. Brewer, Groups in Contact: The Psychology of Desegregation 2 (1984); *see also* Kang, *supra* note 16, at 1160 n.118 (citing similar studies).

[312] *See* Sunstein, *supra* note 99, at 46–96; *see also* Putnam, *supra* note 37, at 177–78; Citron, *supra* note 7, at 81–82.

[313] *See* Sunstein, *supra* note 99, at 46–57.

decrease this risk by increasing cross-cutting relationships.[314] Users will carry with them not only "friends" from a political blog on which they participate, but "friends" from other sites as well. An avid conservative might discover her friend from a gardening forum is a regular participant on Daily Kos, a Democratic site.[315] She might see what her friend has posted on Daily Kos and come to learn more about an alternative viewpoint. She might also choose to criticize what her friend has said at Daily Kos, opening the possibility of dialogue. One study found a strong correlation between Facebook usage and heightened "bridging" social capital, which represents ties between people from different groups who have loosely-connected relationships.[316] By amalgamating cross-cutting relationships, social intermediaries break down the barriers between "echo chambers."

VII. CODE-BACKED NORMS ON THE SOCIAL WEB

Just as social intermediaries act as central infrastructure for building identity and reputation, they also make possible a far greater role for norm development on the Web. No longer do norm success stories need to be limited to large individual sites such as eBay, Wikipedia, and Slashdot. Since social intermediaries offer locations for individuals to display their cross-Web activities, they create opportunities for people to see, analyze, and critique each other's actions. By providing the incentives to use stable cross-Web accounts and build rich reputational data into those accounts, social intermediaries encourage people to take responsibility for their actions.

Except on Facebook, the responsibility taken may be under a pseudonymous identity, with no connection to offline identity. [317] "Responsible pseudonymity" may strike some as an oxymoron. Citing the kinds of incidents of abuse at the social layer discussed *supra*, some leading cyberlaw scholars have suggested we require "traceable anonymity," by which websites would be obligated to record the IP addresses of their visitors.[318] In contrast to "traceable anonymity," as well as Lior Strahilevitz's *How's My*

[314] *Cf.* Kang, *supra* note 16, at 1166–69 (arguing that in contrast to racially segregated offline neighborhoods, cyberspace more easily delivers "disconfirming data" by which racial stereotypes are dispelled).

[315] Daily Kos: State of the Nation, http://dailykos.com (last visited Apr. 15, 2010).

[316] *See* Ellison et al., *supra* note 37.

[317] *See* Kumayama, *supra* note 9, at 442–44 (contrasting anonymity, in which no information related to identity is transmitted, with pseudonymity, which by providing an attached name offers "the ability to accrue reputational capital").

[318] *See* Solove, *supra* note 21, at 146–47; Citron, *supra* note 7, at 123 (advocating requiring website operators to collect and retain visitors' IP addresses); Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. Miami L. Rev. 991, 1031–35 (2004).

Driving? system, the "responsible pseudonymity" encouraged by social intermediaries is not mandatory. Nevertheless, the Social Web will shift the *status quo* toward responsibility, paving the way for additional norm development.[319]

This Part describes the mechanisms for development of code-backed norms on the Social Web. It first describes "reputation scores," which can play a special role in the development of norms. It then reviews how code-backed norms are developed through social intermediaries, with focus in turn on the roles of social intermediary providers, site operators, and end-users. In reviewing these roles, this Part analyzes some of the legal implications of the roles these norm developers play. It next argues that the possibility of "reputation reset" will not undermine norm development. Finally, it contends that the emerging Social Web overcomes the arguments of Neil Netanel and others that the Web is fundamentally inhospitable to norms.

A. Reputation Scores: Quantified Norms

The prior Part discussed how social intermediaries help users build reputations by amalgamating information on their cross-Web activities, personal histories, and interactions with others. These qualitative details are similar to the kinds of information we use in our offline lives to form ideas about people. Social intermediaries can also calculate reputation according to numerical algorithms, producing "reputation scores."[320] Disqus's clout system and IntenseDebate's reputation points are examples of reputation scores. Reputation scores can be expressed as a single number, as on Disqus or IntenseDebate, or by a series of numbers representing different traits, as on Slashdot.[321] These numbers do not merely inform a judgment by others; they represent a quantified, scaled reputation. They have no offline analogue in informal, day-to-day interactions. Their closest offline cousin might be credit scores.[322]

[319] "Pseudonymous responsibility" and "traceable anonymity" are not exclusive, and could work in tandem. Software is being developed by Microsoft and others that would allow users to choose among "identity cards" offering a sliding scale of anonymity, with different levels of identifiability available to be deployed for different purposes. *See* Kaliya Hamlin, *Bending the Identity Spectrum: Verifiable Identity at RSA*, ReadWriteWeb, Mar. 2, 2010 http://www.readwriteweb.com/archives/bending_the_identity_spectrum_verifiable_anonymity_rsa_securtiy_conference.php; *see also* Kumayama, *supra* note 9, at 451–55 (hypothesizing the development of such a system and suggesting legal protections for pseudonymity in such an identity regime).

[320] *See generally* Noveck, *supra* note 295, at 1738, 1752 (discussing reputation scores on Web 2.0).

[321] Reputation scores could also be expressed as letter grades or verbal ratings, as in Slashdot's karma system. Nevertheless, for simplicity, I will describe reputation scores as numbers.

[322] *See* Noveck, *supra* note 295, at 1767, 1782 (analogizing legal protections for credit scores to legal protections for online reputations).

Reputation scores could also be called quantified norms. All reputation score formats discussed previously in this Article are based, at least in part, on user voting. Each vote cast is an expression of what that voter values. Reputation scores, added together across many voters, represent bottom-up group definitions of what behavior is socially valued.[323] For instance, when moderators on Slashdot choose to rate others on whether they are "insightful," they express their judgments about what kind of posts add insight. Compiled across many votes and many users, these ratings form a powerful group definition of what constitutes insightful comments.

Will enough people vote to make reputation scores meaningful? I believe so. First, unlike voting at a ballot box, voting on a reputation score requires only a few clicks. Those who frequent a particular site might find it worth their effort to try to improve the quality of user behavior there. Emotions can also drive rating behavior. In *How's My Driving?*, Lior Strahilevitz contends that drivers would feel emotional satisfaction from telephoning a central hub to criticize (or praise) other drivers.[324] Moreover, social intermediaries and site operators can increase rating behavior by fostering an atmosphere that promotes a sense of community and represents rating as pro-community behavior.[325]

While reputation scores could exist without social intermediaries, they have been impractical for most sites. Without the data points provided by cross-Web activity, any reputation score calculated by a single site would be of low value unless the site was extraordinarily popular. Further, without the assistance provided by social intermediaries, building a system to calculate reputation scores would require too much programming skill for many site operators.

Reputation scores can be attached as "metadata" to user identities, immediately available to be read by a site's software upon a user's login. Of course, software cannot understand all of the nuance behind a reputation score and cannot understand if a particular metric calculates something of value. But a computer can recognize the relative value of a given score within a metric. This makes reputation scores importantly different from conventional offline reputations. Just as social intermediaries provide a central bank for social capital on the Web, reputation scores can become a reputational currency. The easy availability of reputation scores enabled by social intermediaries opens the door to low-effort moderation methods not previously available. These methods are discussed *infra* Part VII.B.2.

Unfortunately, social intermediary providers do not reveal their reputation score formulas. Providers should disclose how their reputation scores are calculated, both to maximize the scores' usefulness and to ensure fairness. Continued secrecy could fuel concerns that social intermediary providers might manipulate reputation scores to serve

[323] *See id.* at 1752 ("[S]ocial software . . . makes it possible for the group or the community to decide on its own 'rating' criteria and implement those by means of the code.").

[324] *See* Strahilevitz, *supra* note 15, at 1731.

[325] *See supra* notes 124–25 and accompanying text (describing Dan Kahan's theories on community-building); *cf.* Zittrain, *supra* note 2, at 147–48 (suggesting that people feel instinctively that Wikipedia owes a duty of social responsibility that other sites do not).

their own ends. While disclosure may not be sufficient to protect consumers,[326] it is a valuable first step.[327] Beth Noveck suggests that reputation providers may lack incentives to disclose their algorithms.[328] If she is correct, then legally mandated disclosure will be necessary.[329]

Reputation score systems should be developed towards providing more nuanced information. The reputation scores generated on Disqus and IntenseDebate are based only on a simple thumbs up/down system, in contrast to Slashdot's multi-factor system. In a commercial setting like eBay, it is fairly clear what a simple "thumbs up" means—good product, timely delivery or payment, etc.[330] However, in many contexts simple popular voting cannot provide useful information since values are too varied.[331] Lior Strahilevitz offers the example of art, in which what is popular among connoisseurs often does not correlate to what is more widely popular.[332]

Fortunately, this limitation is not likely to be permanent. As social intermediaries become more popular and more voters cast their views in reputation score system, social intermediary providers will be able to implement multi-factor rating methods akin to Slashdot's. So long as users are not forced to cast too complicated a vote, such a system would add a negligible cost in additional effort for each rater while adding a wealth of valuable norm-building information.

One could even imagine a "Reputation Score 2.0" system in which users are able to define the very characteristics that would form the basis of their votes.[333] Rather than selecting from a drop-down list of pre-set characteristics, users could choose to categorize their ratings themselves. Social intermediary providers could also offer many

[326] *Cf.* Grimmelmann, *supra* note 12, at 1181–84 (criticizing publicly-disclosed privacy policies as insufficient to protect users of social networks because users may not read or understand the policies and because the policies often do not bind social networks).

[327] *See* Noveck, *supra* note 295, at 1778–79 ("If I am to be accorded a reputational score, I ought to know what the criteria are.").

[328] *See id.* at 1779.

[329] Noveck also suggests a right of correction, akin to protections with regard to credit scores. *See id.* at 1767–68, 1778.

[330] *But cf.* Unsal & Erickson, *supra* note 144, at 104 (suggesting that eBay's system lacks sufficient nuance because it fails to differentiate low-value transactions intended primarily to boost reputation scores).

[331] *Cf.* Strahilevitz, *supra* note 15, at 1762 (suggesting a "How's My Driving? for Everything" approach is only well-suited where norms are universal and efficient).

[332] *See id.* at 1760.

[333] This system would be analogous to the failed "PICS" system for adding meta-tags to websites, which gained popularity in legal circles in the late 1990s. *See* Daniel H. Kahn, *Barriers to the Voluntary Adoption of Internet Tagging Proposals*, 21 Harv. J.L. & Tech. 271, 276–77 (2007).

different reputation score applets, giving users choices that calculate according to different metrics. Additionally, one could imagine social intermediaries adding systems to provide information on the context in which votes are cast. For example, very different considerations likely drive a positive rating at a forum concerning scholarly scientific developments compared to a rating at an irreverent humor site.

B. Sources of Norm Development and Legal Consequences

Norms on the Social Web, like those on Wikipedia, eBay, and Slashdot, will be based on an interplay between site users and the suppliers of the norm-enabling code. By adding social intermediary providers as a new player in addition to users and site operators, social intermediaries add a new layer of complexity to the development of code-backed norms. This Sub-Part will review the role of social intermediary providers, site operators, and users in building norms on the Social Web. In doing so, it will address notable legal aspects of these players' roles in norm development.

1. Social Intermediary Providers

Social intermediary providers like Google and Facebook create the infrastructure necessary for cross-Web norms to develop. In doing so, they define the scope of what is possible on their systems.[334] Since they can define what activity is in-bounds or out-of-bounds for users and site operators, social intermediary providers can potentially exercise significant power over norms.

While Lior Strahilevitz warns against using law to enforce norms that are not universally held,[335] market and technical enforcement of non-universal norms is also perilous. In a competitive market, site operators will be able to select social intermediaries that provide features that best reflect their goals, and users will be able to frequent sites with features they prefer. However, as networked goods, social intermediaries tend towards *de facto* standardization. If a social intermediary gains a large market share, it might attempt to "lock in" users. Social intermediary providers that have large user bases have incentives to prevent easy account transfer.[336] Randal Picker notes that competitors to powerful identity sources are motivated to lower switching costs.[337] As Picker would predict, upstart social intermediary providers, such as JS-Kit and Pluck, offer tools to allow users to connect account from multiple providers, enabling

[334] *See* Lessig, *supra* note 99, at 89.

[335] *See* Strahilevitz, *supra* note 15, at 1762.

[336] *See* Picker, *supra* note 8, at 6–7.

[337] *See* Picker, *supra* note 8, at 7–8.

a form of reputational data transfer.[338] Yet a sufficiently powerful social intermediary provider might use its terms of service, as well as technical controls, to prevent third-parties from facilitating easy switching.[339] Lock-in harms norm development because users become stuck into a limiting social architecture. Rather than liberating users to develop new modes of social governance, a powerful social intermediary with locked-in users becomes a constraining force.

Randy Picker has called for antitrust monitoring to protect account transfer in situations analogous to the one presented by social intermediaries.[340] While antitrust is primarily a tool of economic policy, free speech values support protection against lock-in because social intermediaries exercise significant control over how users identify and express themselves. In today's competitive environment, I have argued that the arrival of social intermediaries obviates the need for property-like protections for reputation portability on the Web. However, if as time passes a single social intermediary provider gains sufficient market power to lock in users, legal reputation portability protection may become truly necessary.

Social intermediaries can take good faith steps to assuage concerns about their potential power. First, they should take a general attitude of openness with regard to their norm-affecting features. They should disclose what behavior is off-limits on their systems and why they have made those decisions. Second, they should readily accept third-party applets. So long as third-party programmers can add features, social intermediary providers do not unilaterally limit the horizons of socializing within their systems. Tight control of third-party applets would undercut the ability for social intermediaries to generate new social structures.[341] Some deletions of applets that harm network functionality or threaten to violate users' privacy will be necessary. Therefore, social intermediaries should disclose the basic standards to which third-party applets must conform, and only delete applets that violate those basic standards.[342] Third, they should not prohibit users from taking their reputational information contained in their accounts to other social intermediary providers, nor should they use technical or legal means to block third-party programs that give users easy technical means to do so. By taking these steps, providers can offer assurance that they intend to protect norm development from the damaging effects of lock-in.

[338] *See supra* notes 251–56 and accompanying text (describing the tools from JS-Kit and Plaxo).

[339] *See* Grimmelmann, *supra* note 12, at 1193 (explaining that Facebook canceled the account of one blogger who used Plaxo's screen-scraper); Picker, *supra* note 8, at 7.

[340] *See* Picker, *supra* note 8, at 8–9.

[341] *See generally* Zittrain, *supra* note 2 (describing the "generativity" of systems that accept all programs and the threat to that generativity entailed by "tethering," by which programs can be deleted or restricted from afar by a central authority).

[342] This proposal, along with James Grimmelmann's proposal that social networks apply "due process" in determining when to delete user accounts, suggest that social intermediaries should adopt a rule of law model. *See supra* note 307 (mentioning Grimmelmann's proposal).

2. Site Operators

Social intermediaries provide site operators strong, flexible tools for moderation. As moderators, site operators can play a significant role in norm development. Without social intermediaries, almost all moderation must be *ex post*, meaning taken with reference to a specific user action. Social intermediaries enhance the power of *ex post* methods by enabling site operators to praise or sanction users with an audience that reaches beyond the operator's particular site. If a site operator deletes a user's comment from his or her site, that deletion could be reflected in the user's history. On the other hand, if the site operator appreciates a user's contribution, he or she can say so in the user's profile.

By creating portable reputation scores, social intermediaries facilitate *ex ante* moderation—moderation without reference to a specific user action.[343] Slashdot's moderation methods could be used on any site, without the need to build a large user base and without the need for dedicated moderators. For instance, site operators can establish limits on who can act on their sites by requiring users to meet a designated reputation score threshold before they can participate. As a softer approach, site operators could follow Slashdot by giving more prominence to the actions of users with better reputations. Also like Slashdot, they could provide individual users control over how other users' reputations affect the display of their user-generated content.

The ease of moderation enabled by social intermediaries has implications for the debate over § 230 reform. Any reduction in § 230 immunity would raise the cost of owning a site because operators would be forced to either engage in greater moderation or risk liability. By lowering the cost of moderation, social intermediaries reduce the burden that diminished immunity imposes on site operators.[344] Nevertheless, immunity should never depend upon engaging in *ex ante* moderation. Private *ex ante* moderation in a competitive marketplace can improve online discourse while leaving open ample opportunities to speak. However, any government encouragement for such moderation violates First Amendment protections against prior restraints[345] and may violate procedural due process requirements.[346]

[343] *Ex ante* moderation was previously possible but prohibitively time-consuming. *See supra* note 86 and accompanying text.

[344] *See* Citron, *supra* note 7, at 124 ("[A]s screening software advances, some classes of online actors may reasonably be expected to deploy the software to limit the amount and kinds of harmful materials on their sites.").

[345] *See Bantam Books v. Sullivan*, 372 U.S. 58, 70 (1963); *Near v. Minnesota*, 283 U.S 697 (1931).

[346] *See Bd. of Regents v. Roth*, 408 U.S. 564, 575 n.14 (1972) (suggesting that speech is a "liberty interest" protected by procedural due process when the state "directly impinge[s]" upon speech, for example through direct prohibition, but not when the state hampers speech indirectly, for example by firing a university faculty member).

3. Elite Users

In *The Future of the Internet*, Jonathan Zittrain writes about how "elite users" on some sites play an important role in site governance.[347] These elites are typically frequent, emotionally-invested users of a particular site. Zittrain praises the role of elite users, writing that they are invaluable in the development of successful participatory sites.[348] Like Wikipedia's administrators and Slashdot's editors, elite users sometimes receive from site operators semi-official status and special powers.[349] For popular sites, the value of elite users as liaisons between operators and typical users is apparent: the ratio of users to site operators becomes too high for them to moderate without help. One solution is to rely on trusted delegates. While social intermediaries ease moderation, they also promote participation. As a result, more sites may choose to deputize elite users.

4. Ordinary Users

Norm development on the Social Web will, at bottom, be driven by ordinary users. Social intermediaries are designed to allow more sites to incorporate user participation and to give users more abilities as they participate. In reputation score systems, even where social intermediary services offer some guidance on how to vote, the votes themselves are a reflection of the judgments of ordinary users. Ordinary users are the means to and the purpose of the Social Web, and they are the reason the multi-layered system of "regulation" it engenders can be called a system of norms.

While norms on the non-intermediated Web are concentrated in individual sites, social intermediaries introduce a second key location for norm growth: "friend" communities. On social intermediaries, clusters of "friends" meet most of the definition of "tight-knit communities" in which norms can grow.[350] They are repeat players since they can access each other's profiles readily, so information related to control flows

[347] *See* Zittrain, *supra* note 2, at 134 (describing important role of early dedicated users on Wikipedia).

[348] *See id.* at 134, 143; *see also* Jonathan Zittrain, *The Rise and Fall of Sysopdom*, 10 Harv. J.L. & Tech. 495 (1997) (lamenting the then-declining role of "sysops," or early forum moderators).

[349] *See also, e.g.*, Posting of Gida Hammami to editorsweblog.org, Gawker Media Network's Efforts to Manage User Comments, http://www.editorsweblog.org/web_20/2009/07/gawker_media_networks_efforts_to_manage.php (July 15, 2009, 16:00 EST) (describing Gawker Media's appointment of "star commenters," who are delegated "mini-moderator" authority over other commenters in the Gawker family of blogs).

[350] *See supra* notes 124–25 and accompanying text (describing tight-knit communities as those (a) made up of repeat players (b) who can identify each other and (c) in which power is broadly distributed and (d) information pertinent to control circulates easily).

easily. Socializing online may also be more democratic and less hierarchical than offline.[351] Therefore, "friend" communities, in addition to individual sites, will be centers of norm development.

C. Reputation Reset, Trolls, and Norm Development

On social intermediaries, individuals can engage in "reputation reset," abandoning accounts with poor reputations freely. This Sub-Part explains reputation reset and how it can assist vigilant individuals in overcoming online embarrassment. It also shows how reputation reset appears to threaten norm development on the Web by facilitating trolls. Nevertheless it contends that social intermediaries provide important context to the actions of users who lack reputations by which the harm from trolls can be minimized.

1. Reset Switch Explained

The biggest challenges for norm development on the Web are the need for a high degree of conformity and the freedom of movement online. If users receive criticism or disapprobation, they can simply abandon the accounts to which the critiques are attached.[352] As when playing a video game, an individual can hit the reset switch on his or her online identity and begin anew. This "reputation reset" undermines the value of social sanctions. As Lior Strahilevitz states, "[o]nline reputation sites suffer somewhat because users with poor reputations can always 'flush' their existing identities and start over with a blank slate."[353]

Not every individual who suffers criticism on social intermediaries will engage in reputation reset. Some people welcome controversy or are indifferent to criticism. Other users, however, will be hesitant to abandon accounts in which they have invested substantial energy to build socially and economically valuable reputational data.[354] For users who have built communities of "friends" in conjunction with an account, abandoning such connections entails real social and emotional costs.[355] Even online

[351] *See* Putnam, *supra* note 37, at 172–73; Rosen, *supra* note 129 (suggesting that the Internet can engender "democratic shaming," in contrast to the hierarchical shunning of the past).

[352] *See* Aresty, *supra* note 12, at 143–45; Lemley, *supra* note 110, at 1269 n.55; Netanel, *supra* note 65, at 432; Noveck, *supra* note 295, at 1746; Rosen, *supra* note 129, at 435. *But cf.* Palfrey & Gasser, *supra* note 277, at 22–37 (indicating that creating social networking accounts makes it harder than ever in the offline world to move to a new location and "start over" as a new person).

[353] *See* Strahilevitz, *supra* note 15, at 1736.

[354] *See* Rosen, *supra* note 129, at 435 (making this point in the context of individual sites); Smarr, *supra* note 5 (discussing difficulty of re-creating personal data).

[355] *See* Yen, *supra* note 24, at 1252 (discussing how, in the days when users typically

norm skeptics Netanel and Lemley admit that leaving online communities can be difficult.[356] The cross-Web nature of communities on social intermediaries only heightens online friendships' value and raises the cost of account abandonment. Nevertheless, the fact remains that users are free to engage in reputation reset, with friend clusters and sacrificed reputation only sometimes serving as a deterrent.

The bright side of reputation reset is that it can provide privacy protection for careful users. Jonathan Zittrain suggests the need for "reputation bankruptcy," by which users can start over in terms of their reputations online.[357] On social intermediaries, people who have been subjected to humiliation or persistent criticism can abandon the accounts under scrutiny. However, when users employ the same account repeatedly, "reputation bankruptcy" requires special vigilance. Complete reputation bankruptcy can be achieved with certainty only if users act totally pseudonymously, having never publicly divulged any offline personal information in connection with the abandoned account.[358] Most individuals are not so careful, nor do they want to be.[359] Therefore, many users will be unable to attain the kind of thorough "reputation bankruptcy" envisioned by Zittrain.[360]

2. The Threat to Norms

While the reset switch offers privacy protection to hyper-vigilant individuals, it also facilitates intentional wrongdoers. In other words, it feeds the trolls. People could intentionally create "single-shot" accounts that they intend to use only once or a few times to engage in what they know to be malicious behavior. In this kind of situation, the troll would not be surprised by subsequent criticism. Instead, the troll engages in what he or she knows to be widely condemned behavior and then avoids social sanctions by

employed email services supplied by their ISPs, leaving an ISP meant leaving behind an identity and friends); Zittrain, *supra* note 348, at 504 n.10 (stating that abandoning friends on individual sites is difficult). Of course, a user could attempt to recreate his or her social connections with a new account. However, this can be an uncertain process, and the difficulties are heightened if the user is trying to hide the connection to the previous account.

[356] *See* Lemley, *supra* note 110, at 1269 n.55; Netanel, *supra* note 65, at 426.

[357] *See* Zittrain, *supra* note 2, at 228–29. I use "reputation reset" instead of "reputation bankruptcy" because Zittrain's term sweeps more broadly than mine.

[358] *See* Grimmelmann, *supra* note 12, at 1193–94 (explaining that portable identity heightens the risks of divulging any private information in connection with an account because data is subject to the privacy protections of the least secure site at which the user employs the account). Telling offline acquaintances of one's online pseudonym also eliminates the possibility of completely reliable reputation bankruptcy.

[359] *See* Grimmelmann, *supra* note 12, at 1151–64.

[360] *Cf.* Kumayama, *supra* note 9, at 428–29, 446–48 (offering more optimistic account of the privacy-protecting value of pseudonymity online).

abandoning the account used. While such trolling was equally possible without social intermediaries, it appears that social intermediaries fail to offer deterrence.

The above analysis might appear to undermine one of my central claims—that social intermediaries will pave the way to a new age of norms on the Web. One might concede that social intermediaries will produce an uptick in socially-approved behavior, but still argue that reputation reset means that there will be no change in the Web's ugly underbelly. Given the need for a high degree of compliance for norm maintenance, trolls appear to threaten the bright future of social governance I describe.

Worse, recall Danielle Citron's concern about the aggregating nature of destructive mobs on the Web.[361] One might worry that just as social networks assisted flash mobs in congregating for attack, social intermediaries will only make the problem worse by paving a direct path from the social network to the site or person to be attacked.

3. Solutions: Contextualization, *Ex Ante* Moderation, and Social Filtering

Fortunately, thanks to social intermediaries, trolls will no longer look like everyone else. Without social intermediaries, there has been no *ex ante* way to distinguish a troll from other users. Operators of sites open to public use have been forced to wait for people to act and then decide whether to intervene *ex post*. When swarms of trolls arrive, the damage has often been done before the problem is detected.

With social intermediaries, as discussed *supra*, responsible users will have incentives to develop positive reputations on their profiles. In contrast, it is easiest for trolls to act with single-shot accounts.[362] The very fact that a person has no history will be an important data point that will immediately make a user suspect. A user's lack of history can put his or her actions in context.[363]

Contextualization, by itself, is insufficient to eliminate all harms.[364] Fortunately,

[361] *See supra* note 57 and accompanying text.

[362] Even if an abusive individual goes to the trouble of building an account with significant positive reputational data before attacking, the time required to do so can itself reduce the frequency of abuse. *See* Citron, *supra* note 7, at 62 n.1 (noting that naturally occurring costs can deter wrongdoing).

[363] The addition of context to user behavior is one of the key changes brought on by the Social Web. *See infra* notes 401–02 and accompanying text (describing Jonathan Zittrain's suggestion that contextualization can help overcome online embarrassment).

[364] For instance, there have been a number of incidents of individuals' home addresses being revealed in threatening contexts online. *See Planned Parenthood, Inc. v. Am. Coal. of Life Activists*, 290 F.3d 1058 (9th Cir. 2002) (en banc) (enjoining publication of certain aspects of the "Nuremberg Files," a website which listed names and address of abortion-providing doctors, with doctors who had been murdered blacked out and doctors who had been injured shaded gray); *United States v. White*, 638 F. Supp. 2d 935, 937 (N.D. Ill. July 21, 2009) (holding that the First Amendment protects the disclosure on a racist website of the name, address, and phone numbers of a juror, with "circumstances strongly corroborative of [defendant's] intent that another person

the moderation abilities provided by social intermediaries can facilitate responsible site operators in minimizing trolls' harmful impact. Site operators can engage in *ex ante* moderation to prevent individuals lacking in reputation from acting on their sites. They can also employ tools to make it especially easy to engage in *ex post* moderation of the behavior of such users.

Additionally, one could imagine Web consumers employing social intermediaries to engage in "social filtering." David Johnson, Susan Crawford, and John Palfrey suggest that while the presumption online has been to accept all content, we might move to a world where people only accept content that comes from trusted sources.[365] While they propose infrastructure-layer verified identity systems as the mechanism for this change,[366] social intermediaries enable the same type of "social filtering."[367] It is possible to imagine social intermediaries configured so that people can browse through them and accept content only from approved friends or others with established, positive reputations. In doing so, individuals could mimic *ex ante* site moderation.

The downside of these approaches is that they punish those who simply are new to an account or who engage in the more salutary forms of reputation bankruptcy. However, not all sites and users will employ social filtering, so new users should have ample opportunities to express themselves and build positive reputations.[368] Just as Wikipedia's "flagged revisions" approach leaves individuals free to move up the ranks of editors,[369] the "probation period" made possible by social intermediaries can represent a compromise between unfettered speech and limiting trolls.

In sum, on sites with social intermediaries, trolls stand out. While contextualization and moderation cannot prevent all intentionally abusive behavior, they should succeed in limiting disruptive behavior sufficiently to enable norms to grow.

D. Conclusion: Rethinking "the Classic Counter-Example"

It is time to rethink Neil Netanel's assertion that the Web is the "classic counter-example" to the type of environment in which norms can shape behavior.[370] The Social

harm" the juror) (internal quotation marks omitted); Citron, *supra* note 7, at 69; Adam Liptak, *Web Sites Expose Informants, and Justice Department Raises Flag*, N.Y. Times, May 22, 2007, at A5, *available at* http://www.nytimes.com/2007/05/22/washington/22plea.html. No amount of contextualization can restore these victims' feelings of security.

[365] *See* Johnson et al., *supra* note 2, at ¶¶ 6–8.

[366] *See id.* at ¶¶ 51–53.

[367] Note that the authors do not use the term "social filtering."

[368] *See* Johnson et al., *supra* note 2, at ¶¶ 70–72 (contending that social filtering will not threaten free speech values).

[369] *See supra* note 158 and accompanying text.

[370] *See supra* note 190 and accompanying text.

Web alters many of the assumptions under which he and others evaluated the Web's capacity for private ordering.

First, the Web is no longer simply too big to handle norms. Social intermediaries enable the formation of smaller "friend" communities, which represent localities of manageable size where norms can develop. Moreover, thanks to social intermediaries, norms scale more easily. Rather than relying on the same haphazard mechanisms for spreading reputation and norms that we use offline, social intermediaries make reputation- and norm-building information easy to acquire and develop.

Second, social intermediaries also help overcome the high cost of norm creation and enforcement. Norm creation on social intermediaries, largely left to individual users, can be as simple as voting on a reputation score or posting an approving or disapproving wall message. Social intermediaries greatly reduce the cost of moderation for site operators, both through *ex post* and *ex ante* methods. In coming years, social intermediaries may also facilitate site operators in giving special authority to elite users, who can act as models and guides for fellow users. Finally, by spreading norm-building information, social intermediaries also allow individual users to choose to enforce norms through purchases and sales, praise or criticism, and friendship or distrust.

Third, social intermediaries facilitate efforts to ensure high compliance with norms. By placing trolls in context as low-value contributors, efforts to block and contextualize their actions become easier. Responsible contributors will be less likely to be scared away by disruptive behavior.

What will the content of norms on the Social Web be? In some contexts, it is relatively easy to predict. For example, on auction sites such as eBay and yellow pages-style sites such as Craigslist, norms will mirror conventional values in commercial settings: Timely payment and quality goods will earn favor, while the opposite will earn scorn. In most other contexts, it would be foolhardy to predict the norms that will develop.[371] Too many varied norms will emerge to be refined into a simple set of predictions.[372] The multiplicity of norms reflects the multiplicity of human values, and as such should be seen as a net positive.

VIII. UGLY SIDE OF THE SOCIAL WEB

Although the growth of norms generally should be welcome as facilitating low-cost social solutions to social problems, it also has an ugly side. As Stanley Milgram's experiments illustrate, social forces can produce cruelty and mistreatment. This Part explores problems that may arise from the expansion of norms on the Web. It first addresses the threat posed by communities that foster anti-social, destructive norms. It then discusses the possibility that portable identity will expand the prevalence of invidious discrimination. Finally, it discusses the dangers of over-enforcement of

[371] *See supra* notes 130–31 and accompanying text (stating that norms scholars have cautioned against assuming that it is too easy to shape or predict the exact content of norms).

[372] *See* Rosen, *supra* note 125, at 427 (stating that in a democratic society, in which status is based on popularity, there is not much consensus on how people should behave).

otherwise-salutary norms. While social intermediaries invite these problems by expanding the role of norms on the Web, this Part also explores their capacity for mitigating the dangers posed.

A. Harmful Norms

Even taking into account the diversity of human values, there are some norms that it is widely agreed are socially damaging, such as norms that promote wanton violence or cruelty. There will be communities on the Social Web, as there are offline, where destructive values will be promoted.[373] Online communities of wrongdoers can congregate on unmoderated sites. To reduce the chance of accidentally rendering themselves traceable, they could also form, as they do now, on sites that do not use social intermediaries.[374] Some sites might even use moderation methods to foster communities with these destructive tendencies.[375]

It is undeniable that destructive norm-communities will emerge. The Social Web is not a panacea. Accordingly, the emergence of social intermediaries should not mark an end to efforts at targeted regulation. When the risk of harm is sufficient, and where regulation is consistent with First Amendment legal requirements and values, we should continue to explore the possibilities of new legal solutions to problems at the Web's social layer.[376]

However, there are several reasons for optimism—reasons to believe that most norm-communities that develop on the Social Web will not be destructive. First, admittedly informal empirical evidence seems to indicate that code-backed norms on the Web have primarily been a positive force. Norms play a positive role on sites like

[373] *See* Johnson et al., *supra* note 2, at ¶¶ 73–74 (noting the risk that formation of separated communities online may encourage the formation of self-contained communities of wrongdoers).

[374] We must be concerned about wrongdoers who are clever enough to evade the detection social intermediaries enable. Nevertheless, these concerns can be overstated. Paul Ohm cautions against excess focus on largely hypothetical "superusers" who can evade nearly any legal and technical restriction. *See* Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. Davis L. Rev. 1327 (2008). Similarly, Jonathan Zittrain states that "it's a cat and mouse game of forensics, and if people don't go to some effort to stay anonymous, it's frequently possible to figure out who they are." Posting of Amir Efrati toWall Street Journal Law Blog, Subpoena Allowed in AutoAdmit Suit, http://blogs.wsj.com/law/2008/01/30/subpoena-allowed-in-autoadmit-suit. (Jan. 30, 2008, 9:08 EST). Just as well-meaning users who wish to remain pseudonymous might accidentally undermine their privacy by revealing identifying data, hapless wrongdoers may do the same. *See* Grimmelmann, *supra* note 12, at 1164–66 (discussing revelations of wrongdoing on social networks).

[375] *See* Citron, *supra* note 7, at 118–19 ("Some website operators function as crowd leaders influencing the mobs' destructiveness.").

[376] It is beyond the scope of this Articles to analyze what the nature of these regulations should be.

Wikipedia, eBay, and Slashdot. These success stories should give us pause before we form too many pessimistic assumptions about the potential prevalence of destructive norms on the Web. Second, social intermediaries give responsible site operators the facilities to eliminate a significant amount of the damage done by aggregated mobs *ex post*. Third, I have argued that while trolls are *ex ante* indistinguishable from other users on the non-intermediated Web, trolls who act under single-shot accounts on the Social Web will appear relatively suspect. If I am correct, then well-meaning Web users will be primed to give their outbursts less attention and less credibility. Fourth, if David Johnson, Susan Crawford, and John Palfrey are correct in asserting that many individuals will turn to social filtering and view only trusted material,[377] the reach of mobs of trolls will be sharply limited. Finally, I have argued that the net effect of social intermediaries will be to create greater feelings that others on the Web are genuinely "people" and worthy of respect.[378] Though there surely will be antisocial norm-communities, the possibility of more fully rounded identities shining through on the Web can mitigate their influence.

B. Status-Based Discrimination

As discussed *supra*, discrimination is a serious problem online.[379] While social intermediaries enable cross-Web identity and norm-development, those same features create the risk of increased status-based discrimination.[380] By identifying themselves according to their offline characteristics, members of traditionally discriminated-against groups risk discrimination online. Moreover, as Lior Strahilevitz states, "majoritarian norms may unduly reflect stubborn biases, like racial, gender, or religious animus."[381]

Further, *ex ante* moderation, which can bar access to sites or create tiered access, may make it harder to determine who is responsible for discrimination. Forbidding access to a person who self-identifies as a minority on that basis alone clearly would violate a cyber-equivalent to Title II of the Civil Rights Act,[382] which forbids discrimination in access to places of public accommodation on the bases of race, color, religion, or national origin.[383] Yet situations can be far more complicated. For instance,

[377] *See* Johnson et al., *supra* note 2, at ¶¶ 6–8.

[378] *See supra* Part VI.D.

[379] *See supra* notes 59–64 and accompanying text.

[380] *See* Citron, *supra* note 7, at 68–69 (stating that because people must establish identities and reputations online to take advantage of the Internet's opportunities, the door is opened to status-based discrimination).

[381] Strahilevitz, *supra* note 15, at 1760.

[382] *See* 42 U.S.C. § 2000a–2000a-6 (2006).

[383] *See id.*; *see also* Tara Thompson, Comment, *Locating Discrimination: Interactive Web Sites as Public Accommodations under Title II of the Civil Rights Act*, 2002 U Chi. Legal F. 409

imagine site operators who, without subjective discriminatory intent, bar people with low reputation scores from acting on their site. If a minority user's low reputation score can be traced clearly to the discriminatory intent of rating voters, what is the site operator's culpability in barring that user from his or her site? Who is culpable if, instead, there is ambiguity in the degree to which the low rating is influenced by discriminatory intent?

Despite these dangers, social intermediaries provide opportunities to reduce the prevalence of status-based discrimination on the Web. In his article *Cyber-Race*, Jerry Kang describes three strategies for overcoming racial (and by extension, other forms of) discrimination.[384] He terms these strategies "abolition," "integration," and "transmutation."[385] By "abolition," Kang means a strategy of hiding race through anonymity.[386] Kang expresses skepticism about "abolition" as a general approach, criticizing it as naive, potentially burdensome on minorities, and doomed by the new (in 2000) emergence of broadband multimedia capabilities.[387] By providing a means for cross-Web multi-media representations of self, social intermediaries continue to undermine "abolition" as a full-scale strategy to combat discrimination online. However, Kang contends that "abolition" is useful in marketplace settings because those who are concerned about discrimination offline can buy and sell in cyberspace, free of that risk.[388] Kang suggests that this solution might be feasible only if rating agencies are formed to assess the reliability of all online transactors; otherwise, he fears anonymous cyberspace exchanges cannot match the kinds of risk-assessment that are possible offline.[389] Social intermediaries, as discussed *supra*, provide the facilities for the risk-assessment that Kang desires without requiring the creation of invasive rating bodies.[390]

Kang is optimistic about the "integration" strategy, and he suggests that cyberspace can increase both the quantity and quality of cross-race interactions.[391] Social

(2002) (contending that websites are places of public accommodation within the meaning of existing Civil Rights Act law).

[384] *See* Kang, *supra* note 16, at 1136–37.

[385] *See id.*

[386] *See id.* at 1136, 1154–59; *see also* Putnam, *supra* note 37, at 172–73 (describing a study showing that as compared to offline, women are less likely to be ignored in online discussions, at least where they hide their gender). Kang sees "abolition" as appealing to those who see racism as inescapable and to those who see color-blindness as the best solution to racism. *See* Kang, *supra* note 16, at 1136.

[387] *See* Kang, *supra* note 16, at 1156, 1158.

[388] *See id.* at 1188–89.

[389] *See id.* at 1191–92.

[390] *Cf. id.* at 1190–92 (suggesting that methods would be needed to protect individuals' privacy from third-party rating services).

[391] *See id.* at 1136, 1160–79.

intermediaries advance several of the factors Kang highlights from social science literature as being important to succeeding with an "integration" strategy.[392] Social intermediaries provide opportunities to encounter "disconfirming data" about previously unknown others that might dispel negative stereotypes. They also offer substantial opportunities for cooperation, for instance in improving and governing discussion forums. Additionally, their "friending" features allow for non-superficial contact among individuals of varying backgrounds.[393]

Kang's third strategy, "transmutation," involves individuals pseudonymously "passing" as members of different racial or gender groups.[394] The goal of "transmutation" is to allow the "passing" individuals to understand the experiences of those in the group they imitate and to learn that identity is distinct from immutable characteristics.[395] Most social intermediaries enhance the "transmutation" strategy by allowing individuals to express pretend characteristics on multiple websites easily.

Ultimately, social intermediaries bear a complex relationship to status-based discrimination. While they raise the risks of the kinds of discrimination about which Danielle Citron and others rightly worry, they also provide opportunities to escape offline discrimination and to promote inter-group understanding. As with other problems at the social layer explored above, the lesson may be that social intermediaries provide new avenues for abuse by the malicious few while assisting the good-faith many—that is, they may offer new avenues for abuse by hardened bigots while assisting most Web users, who act in good-faith, in gaining new understandings of others in society.

C. Over-Enforcement of Norms

Finally, social intermediaries risk inviting over-enforcement of otherwise valuable norms.[396] While many norms are socially beneficial, excessive punishment for their violation is not. Just as we would not want to impose life imprisonment for a parking offense, we do not want someone who commits a minor social infraction to be subject to abject humiliation. By providing ready access to venues to criticize others' actions,

[392] *See id.* at 1165 (citing the following five factors: "(i) exposure to disconfirming data, (ii) interaction among people of equal status, (iii) cooperation, (iv) non-superficial contact, and (v) equality norms"); *see also id.* at 1165–78 (detailing these factors).

[393] It is unclear what impact social intermediaries will have on the presence of equality norms and equality of status, the other two factors cited by Kang as important to integration. Robert Putnam suggests that cyberspace is generally less hierarchical than offline society. *See* Putnam, *supra* note 37, at 172–73.

[394] *See* Kang, *supra* note 16, at 1136–37, 1179–86.

[395] *See id.* Kang notes that this strategy is controversial and has downsides. *See id.* at 1182–85.

[396] *See* Solove, *supra* note 21, at 6–7 (worrying about out-of-control cyberspace "norm police" who punish offline norm violators but can themselves escape responsibility).

social intermediaries make it easier for over-enforcement of norms to occur. Tidal waves of criticism need not come from coordinated mobs of malicious attackers, as described by Danielle Citron. Even well-meaning individuals, acting independently, can also over-enforce norms.

This problem has already manifested without the assistance of social intermediaries. Daniel Solove describes the story of "dog poop girl," a South Korean student who failed to clean up her dog's feces from a subway train when asked to do so.[397] A popular South Korean blog posted a video of the incident, which was then re-publicized in major media outlets around the world.[398] "Dog poop girl," faced with an overwhelming level of criticism, dropped out of her university.[399]

What "dog poop girl" did was wrong, but she did not deserve the scale of punishment she received. Yet it is hard to say that any individual blog, Web user, or news agency that spread the story and criticized the woman is to blame. How can we avoid a massive increase in these kinds of problems on the Social Web?

There are some steps social intermediary providers can take to reduce the chances of a criticism overload. For instance, they could institute "reputation freezes," similar to stock exchanges' "circuit breakers." A "circuit breaker" on a stock exchange halts trading for a period following a massive decline in index values.[400] Similarly, social intermediary providers might automatically prevent more criticism if a user has received too many negative reputation score votes and critical profile comments within a specified time period.

Existing social intermediary features might also assist individuals in overcoming floods of criticism. First, reputation reset, combined with pseudonymity, can protect careful users of social intermediaries. However, if offline identifying data is connected to the shaming, as in the case above, this solution will not be sufficient. Second, social intermediaries can assist individuals by providing them with a central location from which to respond to criticism. Jonathan Zittrain believes that in the future the most reliable solutions to privacy problems will be those that depend upon "more, not less, information."[401] He suggests that contextualization of information can help overcome online humiliation.[402] If he is correct, then social intermediaries can represent an improvement by providing a widely-recognized center of identity from which people can reply to criticism and embarrassing information.

Despite these potential mitigating forces, some people will see a need for

[397] *See id.* at 1–2.

[398] *See id.*

[399] *See id.* at 2.

[400] *See, e.g.*, New York Stock Exchange, NYSE Circuit Breakers, http://www.nyse.com/press/circuit_breakers.html (last visited Apr. 15, 2010) (explaining New York Stock Exchange circuit breaker procedures).

[401] Zittrain, *supra* note 2, at 229.

[402] *See id.* at 229–31.

increased legal and technical privacy protection in response to possibility of over-enforcement of norms. The conversation about the tension between privacy and responsibility will become increasingly important on the Social Web.

IX. CONCLUSION

Social intermediaries represent a substantial step toward a more responsible Web. Through social intermediaries, people can maintain consistent identities across many websites. These new application-layer systems for portable identity will mean that social forces can shape behavior on the Web far more than was previously possible. Social intermediaries also make it possible for users to aggregate reputational information developed from across the Web. Because Web reputations will be easier to build and more valuable, many more users will be motivated to engage in socially valued behavior so that they can earn the benefits of the emerging reputation economy. Websites will be able to open the door to user participation more easily and more flexibly, without fear of inviting only a "flame-ridden cacophony."[403]

Social intermediaries provide the "social glue" that can enable the Web to become a place of robust, contextual, multi-faceted norms. Social intermediaries promote an atmosphere in which people recognize each other as fully rounded individuals who are worthy of respect. In the absence of legal protections online, social intermediaries facilitate bottom-up responses to problems at the Web's social layer. When the norms that emerge fail to curb social-layer problems sufficiently, we should consider regulatory responses.[404] Nevertheless, the new possibility of social solutions should at least give us pause before we adopt Danielle Citron's "aggressive pro-regulatory posture."[405]

While offering an alternative to legal responses to social-layer problems, social intermediaries also introduce novel regulatory challenges. In considering whether to create new privacy baselines, regulators should aim to leave users free to take full advantage of the opportunities for reputation-building and accountability afforded by social intermediaries, while considering how best to protect them from being pushed into ceding privacy without their understanding and consent. Insofar as these goals are in

[403] Netanel, *supra* note 65.

[404] As Robert Ellickson concedes, law is preferable even in a high-norm environment when established norms fail to support important values, including protecting fundamental rights and achieving distributive goals. *See* Ellickson, *supra* note 107, at 283–84. Danielle Citron argues that, in implementing the cyber-civil rights agenda she advocates, law's expressive power can promote understanding of the particular harms online harassment causes to women. *See* Citron, *supra* note 130. While I am more hesitant than Citron to intervene legally in the Web's social layer, I believe she is absolutely correct to treat the law's expressive value as an important consideration in regulatory efforts. As the Web becomes more social, norm management (though necessarily imprecise) must move to the forefront of any discussion of regulatory strategy.

[405] Where norms successfully promote positive social results, introducing a new emphasis on legal rewards and punishments may actually undermine cooperation and trust. *See* Kahan, *supra* note 128.

tension, further discussion will be needed on the correct balance between privacy and accountability. Social intermediaries also introduce a host of regulatory challenges unrelated to privacy, including issues of commercial honesty, market power, antisocial group formation, discrimination, and over-enforcement of norms.

Portable identity has arrived without legal mandates or changes to the Internet's core architecture. Social intermediaries undercut the assumption that the Web is by nature inhospitable to norms. Which of our fundamental beliefs about the Web's social structures will be shaken tomorrow? Regulation of the Web must, as best as possible, account for its mutable nature.