Community Node-Based User Governance (CNBUG): Applying Craigslist's Techniques to Decentralized Internet Governance

Alice Goldmann
Benjamin N. Cardozo School of Law

ABSTRACT

In the *Accountable Internet: Peer Production of Internet Governance*, Cyberlaw-scholars Professors David R. Johnson, Susan P. Crawford, & John G. Palfrey Jr. suggest decentralized governance and user accountability as a means of governing the Internet. While advantageous over existing centralized models, Peer Production model also suffers from significant practical shortcomings that would make it unlikely to be adopted as a global means of Internet governance. A new model, Community Node-Based User Governance (CNBUG), inspired by Peer Production's decentralized model, consists of three principal components that establish its effectiveness: decentralized user-dependent governance, geographic nodal-centered communities, and quorum flagging, similar to that employed by Craigslist.org, an online community information Web site. These three components work together to establish a means of Internet governance that unlike its predecessors, does not chill speech or isolate users, integrates decision-making accountability, allows for the participation and integration of developing nations, represents global community standards, allows for concurrent online and territorial enforcement, and protects users from bad actors; all while preserving the Internet's fundamental purpose and nature, and also leaving intact its considerable business and technical infrastructure.

Community Node-Based User Governance (CNBUG): Applying Craigslist's Techniques to Decentralized Internet Governance

Alice Goldmann
Benjamin N. Cardozo School of Law

Should the Internet be Governed?

Cyberscholars, governments and users have been faced with the looming question of whether the Internet can and should be governed. Since the Internet's inception and its subsequent evolution into an inexpensive and omnipresent means of global public communication, users have been resistant to the idea of being governed online. When President Clinton signed the *Telecommunications Act of 1996*[1] into law, John Perry Barlow responded with his now infamous *A Declaration of the Independence of Cyberspace*[2]. In it he decreed that territorial governments have no business governing the Internet, and that it would be governed from within.

For years, various governments have attempted to govern the Internet through the creation of new laws, online borders, and extraterritorial enforcement, yet very few have succeeded. At the same time, there has been a proliferation of 'bad actors'[3] online, and it has become evident that something must be done to protect users.[4]

The Accountable Internet: Peer Production of Internet Governance[5] (and its follow-up submission to the International Telecommunications Union Workshop on Internet Governance[6]) attempts to solve the problem of governing the Internet by proposing a new model of Internet governance that is meant to supplant the two existing models known as the Benevolent Dictatorship Model ("Benevolent Dictatorship") and the Democracy Model ("Democracy")[6]. The *Accountable Internet*'s proposed Peer Production Model ("Peer

---

[1] See Telecommunications Act 1996, Pub. LA. No. 104-104, 110 Stat. 56 (1996) http://www.fcc.gov/telecom.html (last visited, August 10, 2006).
[2] A Declaration of the Independence of Cyberspace http://homes.eff.org/~barlow/Declaration-Final.html (last visited, August 10, 2006). Specifically, Barlow's manifesto was in response to the Communications Decency Act, Title V of the Telecommunications Act. See http://hotwired.lycos.com/wired_online/4.06/declaration/ (last visited, August 10, 2006).
[3] See Footnote 5, Pg. 4, ¶4.
[4] http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf (FBI's Internet Crime Complaint Center cites that from January 1, 2005 to December 31, 2005, complaint submissions increased by 11.6% from the previous year. Dollar loss was pegged at $183.12 million. (Charts for dollar loss available in the above pdf for 2001 – 2005) (last visited, August 10, 2006)..
[5] *See* David R. Johnson, Susan P. Crawford and John G. Palfrey, Jr., *The Accountable Internet: Peer Production of Internet Governance*, 9 VA. J.L. & TECH. 9 (2004).
[6] *See* John G. Palfrey, Jr., *Submission to the Workshop on Internet Governance February 26 – 27, 2004*, International Telecommunications Union, Geneva, Switzerland.

Production")[7] rejects the idea of a centralized Internet government inherent in Benevolent Dictatorship and Democracy. Instead it proposes that each individual user be responsible for governing the Internet.

Building on the strengths and advantages of Peer Production, this paper proposes Community Node-Based User Governance ("CNBUG"), a new model that maintains the decentralized aspects of Peer Production while enhancing it with the administration aspects of Craigslist.org ("Craigslist"), a community information and classifieds Web site (see Appendix A).

Three Models of Internet Governance

While all three models of Internet governance reviewed in *The Accountable Internet: Peer Production of Internet Governance* [5] embody certain advantages, they also suffer from significant practical shortcomings that would make them unlikely to be adopted as a global means of Internet governance. Note that these three models apply to governing the Internet as a whole rather than on a per-Web site basis.

Benevolent Dictatorship Model

A walled garden is a pre-defined area on the Internet that is subject to the control of an overseer, referred to as the 'benevolent dictator' ("dictator"). Walled gardens can be private such as AOL.com, where users that choose to participate in AOL's online community agree to subject themselves to its rules; or public, such as exists in the Peoples Republic of China, where online communications within the country are regulated internally, and those originating from outside its geographic borders are filtered by a customized firewall[8].

In a Benevolent Dictatorship, the Internet is a walled garden where all those inside the wall are protected by the dictator but are also subject to his/her discretion, rules, policies, and enforcement control. Users typically participate in the walled garden with the expectation that the dictator is ensuring that unsuitable content and malicious actions are not occurring within its walls. In certain private sector controlled walled gardens, such as

---

[7] Also known as decentralized action.
[8] Clive Thompson, Google's China Problem (and China's Google Problem), New York Times Magazine, April 23, 2006.

AOL, users defer to the dictator's technological prowess in keeping their Internet safe and free of problems, indecencies, viruses, and spam. In furtherance of this goal, AOL provides its subscribers with email filtering, firewalls, parental controls, anti-virus and anti-spyware software, identity theft protection, and an army of overseers (employees) entrusted with keeping the walled garden safe and secure[9].

A longstanding problem with the Benevolent Dictator Model is its historical reputation for dissatisfactory customer service. Even though participants can report non-compliant content to the dictator, each posting must be reviewed on an individual basis to determine whether or not it is compliant with corporate policy and the law. This approach is inefficient and expensive: "Although users registered a steady stream of complaints, they saw little reduction in bad behavior since individualized ad hoc attention to each reported problem could not put a significant dent in wrongdoing."[10] To stay in business, the company in question had to eventually move away from the Benevolent Dictator Model, by shifting power and decision-making to its clients[10].

While safe within their walled garden, the Benevolent Dictatorship's participants effectively consent to the dictator's unbounded authority to shape their Internet experience. Their 'best interests', and thus the content and information they are able to access online, are determined according to the dictator's discretion. Users often do not even realize that the content they are exposed to is filtered, missing, or censored[11], as the dictator has full discretion and capability to restrict information without notice, accountability, or scrutiny.

Despite the private Benevolent Dictator having so much unaccountable control, US courts have nonetheless found that by participating in a private enterprise such as an online walled garden, subscribers implicitly consent to such rules. Where the private enterprise is not a monopoly, US courts have been reluctant to void the enforceability of boilerplate contracts, suggesting instead that the consumer had the option to accept those terms or go

---

[9] See http://discover.aol.com/aolfeatures.adp (last visited, August 10, 2006).
[10] The Cardozo Law School's Floersheimer Center for Constitutional Democracy's Occasional Paper #2, January 2005.
[11] *American Library Association v. United States*, 201 F. Supp. 2d, 401, 446.

elsewhere[12]. In China, the Chinese government has cited morality and public welfare in justifying their strict and yet undefined rules on Internet content[8].

Democracy Model

In a Democracy, users elect a body of representatives that is entrusted to govern the Internet[5]. Democracy has the advantage of reflecting the will of the voters and, unlike in a Benevolent Dictatorship, makes the decision-makers periodically accountable for their actions. Ideally, users can elect a body of representatives that reflect their values and take action on their behalf, instead of relying on the judgment of a pre-appointed unaccountable governing body.

One of the biggest challenges evoked by Democracy is compliance with differing global values, customs and attitudes. Even if a representative body were successfully elected to govern the Internet, it would have the impossible task of establishing a set of uniform global Internet rules that would be able to satisfy the enormous variations and often passionately and violently conflicting contradictions of community standards[13] across the globe.

For example, while some countries legally mandate sexual education classes for children in public school[14], the mere suggestion of sexual education would be unthinkable in certain cultures and belief systems. A globally elected body of representatives would have difficulty passing judgment on a safe sex Web site for teenagers, or an AIDS and HIV or birth control information Web sites for adults, that would satisfy communities that view this information as essential and those that are adamantly opposed to its open availability and dissemination.

In China for example, Web sites about Falun Gong or the Tiannamen Square Massacre are strictly prohibited, with violators imprisoned for posting or even viewing such

---

[12] *Caspi v. Microsoft Network, L.L.C.*, 732 A.2d 528, 531, (N.J. 1999).
[13] Community standards are the unsaid rules by which any community conducts itself. See *ACLU v. Reno*, 217 F.3d 162.
[14] Britain: Sex Education Under Fire: United Nations Educational, Scientific, and Cultural Organization, http://www.unesco.org/courier/2000_07/uk/apprend.htm, (last visited, August 10, 2006).

content on the Internet[1015]. In Iran, filtering extends to Farsi-language blogs, email, and online discussion forums with prohibited content, including but not limited to gay and lesbian, politically sensitive, and women's rights Web sites[16]. Both exemplify content that does not typically offend the community standards of many other countries, and demonstrates how on a global scale, the enormous variation of social and religious values would necessitate an infinite set of diverse community standards.

In an online Democracy, problems would also arise if the majority of users were to elect a particularly conservative Internet government that would chill online content and speech; or an overly liberal government that would permit content and speech that some communities found objectionable (or even illegal) such as the sale of Nazi memorabilia in France[17].

Paradoxically, a freely elected Internet government could potentially create a global imbalance of representation, resulting in global rules and standards made by the select few, likely the richest economies or most developed nations. Certain localities that are currently restricted from online participation due to the digital divide[18] could be prevented from voicing their needs[19]. By the time these localities established a significant online presence, they would be forced to conform to an existing governance infrastructure. The less powerful participants would inevitably resent global rules made on their behalf but without their input, which would cause conflicts rather than lead to cooperation and compliance[20].

Finally, even if it were elected democratically, certain nations could refuse to recognize the rulemaking and decisional power of a global Internet government. Since it

---

[15] For more information on world-wide content monitoring and filtering see http://www.opennetinitiative.net/modules.php?op=modload&name=Archive&file=index&req=viewarticle&artid=1 (last visited, August 10, 2006).
[16] Internet Filtering in Iran in 2004-2005: A Country Study http://www.opennetinitiative.net/studies/iran/ (last visited, August 10, 2006).
[17] *Yahoo! Inc. v. La Ligue Contre Le Racisme*, 433 F.3d 1199, 1202 (Prohibition on sale of Nazi Memorabilia in France).
[18] 'Digital Divide' refers to the gap between those able to benefit from digital technology and those who are not. See International Telecommunications Union: http://www.itu.int/ITU-D/digitaldivide/ (last visited, August 10, 2006).
[19] See International Telecommunications Union: Statistics on Worldwide Internet Access http://www.itu.int/wsis/tunis/newsroom/stats/ (last visited, August 10, 2006).

would be unlikely that an Internet-based government would have the authority and police power to enforce its rulings, it would have to rely on traditional territorial regimes for such enforcement. As it stands today, due to conflicting laws, territorial governments do not always have their rulings in Internet-related matters enforced by other governments[21].

Even if a group of countries were to successfully create and implement a Berne Convention-type treaty[22] to enforce the rulings made by the Internet government, any nation that did not join the treaty would become a global haven for bad actors and thus create a 'race to the bottom'.

Peer Production Model

Peer Production eschews the idea of a centralized Internet government, and instead lets individual users to govern the Internet on their own behalf, by enabling them to permit or block contact from other users. By controlling their personal exposure to informational flows, individual users exclude bad actors that contact them, while also lowering the danger of 'chilling' content on the Internet as a whole. In determining whether or not to permit a contact to reach a user, Peer Production usually relies on a 'trust' system, built on the recommendation of others that are somehow trusted to certify the value of a communication.[5]

Despite Peer Production's revolutionary shift to a decentralized model, it suffers from several significant disadvantages that make it an unlikely candidate for Internet-wide implementation. Conceptually, a collective of individuals, each working on their own, are inefficient in governing a complex system like the global Internet[23]. As well, in creating a self-imposed 'microcosmic walled-garden', individual users could enable a 'reverse-chilling'

---

[20] Ian King, Internet Governance: An Analysis of the Need for Change, 19th British and Irish Legal Educational Association (BILETA) Annual Conference, 2004/.
[21] *La Ligue Contre le Racisme et l'Antisemitisme, et al., Petitioners v. Yahoo! Inc.*, 433 F.3d 1199, 1221 (2006) US court refused to enforce ruling of French court prohibiting certain content on Yahoo because it violated the first amendment.
[22] The Berne Convention http://www.wipo.int/clea/docs/en/wo/wo001en.htm/ (last visited, August 10, 2006).

effect, where the user would inadvertently deprive themselves of content they would want to see, but could not, because they unknowingly set overly broad filtering criteria[24].

Another weakness of the Peer Production's trust-based system is that it hinders the interconnection of strangers — one of the Internet's most fundamental and beneficial attributes. The Peer Production trust-based system would create a barrier to online participation, as new users would have to already 'know' someone and be 'trusted' before being permitted to participate[25,5].

The proliferation of the Internet has allowed for communication between users thousands of miles away, without delays or substantial costs. It enables people to create a virtual online identity (MySpace, Friendster), make romantic real-life connections (Match, Lavalife), buy and sell (eBay, ioffer), blog (blogger, livejournal), and be involved in infinite other online 'actions' on a global scale. In contrast, Peer Production endorses a system that requires authentication prior to intra-user communication. Limiting online communications between strangers simply because trust requirements have been set too stringently, or because intra-user trust has not been established, could create user isolation or, possibly, alter the fundamental nature of the Internet as an open global communications medium[26].

An implementation of Peer Production that relied on other users' recommendations of trust instead of one from a neutral third party could be insecure. Even in an online system where trust is 'earned', nothing would prohibit trusted users from later emerging as bad

---

[23] Hofmann, Jeanette (2005) "Internet Governance: Eine regulative Idee auf der Suche nach ihrem Gegenstand", in: Gunnar Folke Schuppert (Hrsg.): Governance-Forschung – Vergewisserung über Stand und Entwicklungslinien, Band 1 der Reihe Schriften zur Governance-Forschung", Nomos-Verlag: Baden-Baden, S. 277-301. (Hofmann warns that Peer Production self-governance might run up 'against the limits of its regulatory capacity'.)
[24] For example, disallowing content containing the word 'breast' will omit results containing 'breast cancer' and 'chicken breast', neither of which is sexually suggestive.
[25] This would especially affect users that were 'coming out' of a digital divide situation and who would likely not know anyone online to provide them with the required references.
[26] As evidenced by the philosophy behind the Internet Protocol: http://www.ietf.org/rfc/rfc0791.txt (last visited, August 10, 2006).

actors[27]. By the time a once trusted user committed an attack and appropriate corrective action was taken, the damage would have already been done.

Worse still, if the Peer Production 'trust' model were implemented on a network consisting of open connections between numerous trusted users, the effect of just one bad actor could swiftly overwhelm the entire network with devastating results. There exists no foolproof or definitive way either online or offline to forever ascertain someone's character. Moreover, trusting a stranger online because they have established trust with someone you trust does not serve to eliminate this problem. There is no guarantee that your 'friend' has exercised diligence or discretion in opting to make a connection. For instance, on the popular social networking site MySpace.com, users purposefully accept friendship requests from as many people as possible for the sole purpose of feigning online popularity[28]. Often they have absolutely no reference point for accepting a particular user into their personal network, as the request for being 'added' as a friend is completely random and the users do not know each other beforehand. Online, a user can make friends with hundreds of people and then purposefully send them spam, or even a virus, which would then get distributed across their 'trusted' user base[29]. A trust-based black-and-white list system is unlikely to prevent bad actors from participating on the Peer Production Internet.

The deficiencies of the above-described governance models illustrates the inherent difficulties in creating a means of global Internet governance that could reconcile numerous incongruous requirements, such as avoiding chilling speech and user isolation, ensuring accountability, including developing nations, representing global community standards, allowing for concurrent online and territorial enforcement, and protecting users; all while

---

[27] eBay Inc. is an example of a trust based (but not reliant) transactional system. For every transaction conducted on eBay, users may opt to leave each other feedback regarding the success of the transaction. Some bad actors were able to effectively circumvent the eBay trust system by spending a few months building up positive feedback for sales and purchases completed successfully, basing this positive feedback on small low priced or fictional transactions. After a few months and a full portfolio of positive feedback, these bad actors have been known to start aggressively selling more expensive items that were either broken or nonexistent.

[28] http://www.usatoday.com/tech/news/2006-01-08-myspace-teens_x.htm (last visited, August 10, 2006).

preserving the Internet's fundamental purpose and nature, and also leaving intact its considerable business and technical infrastructure.

Proposal for a Fourth Model of Internet Governance: Community Node-Based User Governance

The method of content administration that exists on Craigslist (see Appendix A), in conjunction with the decentralized advantages of Peer Production, evokes a fourth model of governance that I have named **Community Node-Based User Governance ("CNBUG")**. CNBUG consists of three principal components that establish its effectiveness: decentralized user-dependent governance, geographic nodal-centered communities[30] and quorum flagging.

In a CNBUG implementation, real life localities would exist on the Internet as community 'nodes', where a node can be a city, state, country, or a permutation of these[31]. Each node's participant makeup would mainly comprise that of the node's corresponding geographic location.

CNBUG's decentralized governance takes the form of providing decisional and enforcement powers to all users that choose to participate in a CNBUG node. Node participants govern by quorum flagging, which is a type of voting. When community node participants encounter content (i.e., text, an image, or a subject category) that they believe is inconsistent with their node's norms, terms of use, or laws, they can voice their disapproval by clicking a button that corresponds to a reason why the post should be removed or reviewed ('flagging the post'). The post is not removed unless its predefined flagging threshold has been met (i.e., flagged by a predefined quorum of users). After the flagging threshold has been reached, the person who posted the offending content receives an email notifying them that the posting has been removed and for which violations (i.e., which flag has triggered the post's removal).

---

[29] In a network where all participants are connected to each other, a virus or spam sent to one user would potentially have the ability to affect every interconnected user.
[30] A geographic node can be replaced with a professional organization node. For the purposes of this paper, I will only discuss the applicability of a geographic scenario, but the general aspects and ideals would be applicable in both situations. Examples of applicability will be stated as they apply throughout this paper.

How CNBUG Compares to the Other Three Models

Even though it looks quite simple, CNBUG provides a powerful and easily understandable governance mechanism that embodies positive elements from Benevolent Dictatorship, Democracy, and Peer Production, while creating an entirely new model. Unlike Benevolent Dictatorship and Democracy, CNBUG does not rely on a central body to govern the Internet. Like Peer Production, it utilizes a decentralized form of governance, empowering individual users to govern their Internet node — by independently deciding what content should or should not be removed from their online community. In essence, CNBUG is sufficiently flexible to allow users to govern any type of content that a particular online community would deem necessary to regulate via collective action.

The table in Appendix B compares the principal advantages and disadvantages of the aforementioned Internet governance models, as well as the Craigslist community service.

CNBUG versus the Benevolent Dictator Model

In a private Benevolent Dictatorship such as AOL.COM, the walled garden's rules take the form of the 'terms of use' that outline acceptable and unacceptable behaviors. When the terms of use in a private dictatorship are violated, a concerned user must bring the violation to the attention of the dictator's representative and then wait for a response and/or corrective action, if any.

In AOL's walled garden, the dictator (via employees that act as administrators) enforces the terms of use by warning, penalizing, or banning users for certain behaviors. As in a private Benevolent Dictatorship, CNBUG would also incorporate a written 'terms of use' defining acceptable and unacceptable community behaviors. However, unlike the Dictatorship, CNBUG enables participants to make 'collective enforcement decisions' independently of any overseeing body. The substantive difference between an implementation of CNBUG and a Benevolent Dictatorship is that CNBUG allows participants to 'vote' (via flagging) on issues that directly affect them and their community, thus enforcing their community's norms. In contrast, on AOL, users do not have the ability to govern the walled garden, instead relying on the dictator. When AOL's employees do

---

[31] Or a professional organization.

govern (i.e. remove content that violates their terms of use), they are required to do so according to the company's policies rather than community's norms. Hence, when a violation occurs that is not against corporate policy, service administrators might be slow to act, or not act at all.

Such a situation occurred in *Zeran v. AOL*[32]. In *Zeran*, an AOL member began posting offensive pro-Oklahoma City bombing t-shirts for sale, and provided Zeran's name and contact information, urging people to call him with orders. Resultantly, Zeran became the victim of thousands of harassing and threatening phone calls, appealing to AOL to remove the posts and suspend the violator's account. As AOL was slow in deleting both the posts and the offender's AOL account, the postings and the harassment continued. The same post on an implementation of CNBUG would have likely been flagged immediately on account of its tasteless nature, thus sparing Zeran a bulk of the harassment he suffered waiting for AOL to take it down. The post's removal would be based on its non-compliant content, and would not have to be illegal or even explicitly in violation of the community's written terms of use in order to be removed.

Since CNBUG allows for governance according to community's norms as well as the law, there is no requirement that a removal action be justified in compliance with a policy. Under Lawrence Lessig's model of behavioral regulation[33], Lessig distinguishes between normative punishments as those enforced by the community and legal ones as those enforced by the government. By allowing both types of enforcement to take place concurrently, CNBUG permits an increase in the effectiveness of legal enforcement, because it frees up law enforcement officers from dealing with insignificant matters so they can focus on egregious violations.

For example, experienced users might be familiar with postings that embody certain Internet scams, which might be non-obvious to less savvy users. Since CNBUG's first line of defense is flagging, users can promptly remove such postings on behalf of their community before others even have a chance to be victimized. Such an approach, while preventing

---

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

would-be victims from falling prey to the scam, does not preclude coexisting legal enforcement by local authorities, which might take place without notification to a CNBUG node's participants[34].

On an implementation of CNBUG, while the rules might be echoed in the terms of use ('thou shall not infringe on they neighbor's copyright'), it is the users that ultimately determine when and if these rules are enforced online, thus relying on fluid norms rather than just law for the purposes of governing their community. For example, if Paris, France's users have refused to enforce copyright law by not flagging posts that contained unauthorized reproductions of copyrighted material, they would simply not be flagged. No centralized Europe-wide or France-wide decision is made or required and the decision itself would be reflected in the community's unwillingness to fulfill the flagging threshold that would remove the legal violation.

If an insufficient number of users flag a post and the pre-determined flagging threshold has not been met, then the post would not be removed until it expires[35] or unless a legal action is independently forthcoming. CNBUG's means of normative enforcement would not however, prevent the lawful intellectual property holder from bringing a legal cause of action for copyright infringement.

Unlike a Benevolent Dictatorship, which conceptually, is not obligated to have accountability, CNBUG integrates decisional accountability into every removal action via a peer-review mechanism (manifested as quorum flagging), which requires a certain pre-defined threshold to be met prior to allowing the posts' removal. By distributing the responsibility to flag content among multiple users, the abuse of power is less likely.

Not only is CNBUG's flagging threshold set automatically but also, additional technological safeguards can be integrated into the system to ensure that any one user

---

[33] *See* Lawrence Lessig, Code and Other Laws of Cyberspace, 192-193 (1999).
[34] Coexisting where the CNBUG participants could flag a post and, in addition, a legal action could be taken where applicable.

could not repeatedly flag a post. These safeguards further serve to validate the removal decision and reflect the true will of the community rather than that of a pro-active minority forcing its radical values on others. Since an insufficient quorum could not remove a post, this creates a strong implication that it is not offensive to the community's norms.

While the protection of the walled garden is solely entrusted to the dictator, under CNBUG the ability to protect a nodal community is distributed equally among all its participants. A decentralized system allows for faster response to problems because, unlike in a hierarchical centralized private entity, community participants are not required to wade through several bureaucratic layers in order to comply with a corporate policy before making a decision. CNBUG permits participants to respond by voting as soon as they spot a violation, whereas a complainant in a walled-garden would be powerless to remove a post, even if it affected them directly.

Despite relying on decentralized enforcement, CNBUG is not dependent on full member participation. The system would still function if particular users were always proactive (consistently flagging posts that do not comport with the rules); if certain users were flagging just some of the time (removing only the posts with egregious violations or that were personally offensive); or even if the majority was never flagging (in case the subject was obscure or users were apathetic — 'someone else will do it'). In CNBUG, users are constrained from acting only by their own willingness to do so, and not because they are lacking the ability to act. Hence, proactive and interested users can reliably act on behalf of and in the best interests of their community.

CNBUG versus the Democracy Model
One of the main problems faced by Democracy would be implementing governing Internet standards on a global scale. Taking into account that even in the United States these standards vary considerably within states (New York City v. New York State

---

[35] For example, on Craigslist, the flagging guidelines prohibit posts that contain link referrals, designating them as an example of content that should be flagged under 'spam'. However, if no users flag these posts, they simply remain on the system, the implication being that they are either comport with the local community's normative standards, are inconsequential, or have simply gone unnoticed by those who would otherwise flag them.

standards)[36] and between states (Utah v. Massachusetts)[37], the possibility of implementing a global standard that could satisfy all participating nations would be nearly impossible (Singapore[38] v. Holland).

CNBUG solves this problem by creating communities that are online manifestations of geographic locations[39]. Such a means of online community representation is effective for two principal reasons. First, people's community standards are significantly linked to their geographic origins[40]; and second, because laws are linked to the physical locality where they are meant to rule. Having online communities exist as city/state nodes permits participants from those localities to project their community's norms and laws onto the Internet and vice versa. Therefore, a poster on the Kansas City node searching for marijuana would likely be subject to a stricter community standard than one on Amsterdam's node because of the latter city's more liberal laws and social norms[4142].

Unlike Democracy, CNBUG would accommodate users and communities stuck in the digital divide. Because CNBUG communities exist as online manifestations of their physical locations, no existing community can make decisions or set standards on behalf of others. As each nodal community grows and establishes a firmer online presence, they can apply their own norms, even if they are nested within a larger online community. With the narrowing of the digital divide, new participants would have the opportunity to establish an online presence that is reflective of their norms and laws, rather than be forced to conform to pre-existing regulations.

---

[36] NYC is considered progressive while the rest of the state is more conservative.
[37] Utah is governed with a significant participation of the Mormon Church, whereas liberally inclined Massachusetts is the first US state to legalize gay marriage.
[38] http://www.opennetinitiative.net/studies/singapore/ (last visited, August 10, 2006).
[39] Also, conceivably professional associations, international standards bodies and similar closed-membership groups that are governed by by-laws and utilize proprietary enforcement mechanisms can use CNBUG online governance model.
[40] Or in a professional organization context, the association memberships' community standards.
[41] Netherlands Ministry of Foreign Affairs: A Guideline to Dutch Policy on Drugs http://www.minbuza.nl/default.asp?CMS_ITEM=6D389503422F4A58867070C835BCF837X1X55968X17 (last visited, August 10, 2006).

Even if users were to elect a global Internet government, there is no guarantee that territorial governments would recognize or enforce this government's power or decisions. This danger is not at issue with CNBUG because it does not remove legislative, jurisdictional, or enforcement power from territorial governments. CNBUG simply empowers individual users to govern their community node according to norms that coexist alongside legal enforcement. Giving users normative enforcement power is also effective where societal norms and the law overlap, as bad actors can still be punished by both[43]. Any government, online or offline, typically only has the time and capability to address a limited number of pressing issues. Hence, the creation of a means to empower individuals to govern on matters that affect them personally removes the need to defer to a central online representative to govern the Internet. CNBUG is a viable manifestation of this power, both in the acceptance or rejection of individual content and, cumulatively and indirectly, managing the Internet as a whole.

Creating online communities that correspond to territorial localities significantly reduces the fundamental confusion as to choice of law applicable in legal enforcement determinations, such as notice and jurisdiction (i.e., in the US, fulfilling minimum contacts for personal jurisdiction[44]). For example, a node in Winnipeg, Manitoba, Canada is clearly subject to Canada's federal laws, Manitoba's provincial laws, and Winnipeg's municipal laws, in addition to the normative standards of all three[45]. CNBUG would adopt Craigslist's policy on encouraging users to participate only on the online manifestation of their territorial community[46], although it would not prevent them from participating in other communities of

---

[42] In a professional association context, a book on the history of evolution posted in a forum for history professors might not be flagged, but the same book posted on a religious elementary school teacher's association Web site might be removed, especially if it were not posted in a critical context.

[43] For example, if a user is posting pornographic photos in an inappropriate category, community users might flag this post. If the photo involves minors, law enforcement authorities would not be precluded from involvement, even if such content were already flagged.

[44] *International Shoe Co. v. Washington*, 326 U.S. 310 (1945).

[45] Similarly, professional associations usually deploy proprietary regulatory and ethical frameworks enforced by both state regulators and their professional community's standards.

[46] See: http://www.craigslist.org/about/help/reasons.html#wronggeo (last visited, August 10, 2006).

their choice. Participation within one's online community node creates knowledge of the community's norms, as well as familiarity with its laws, rules, jurisdiction, and enforcement[47]. Even participation within a community node that was not one's own, would nonetheless create the expectation of being subject to that community's norms and laws. An American, posting on Sydney, Australia's node, would know by virtue of participation on that node that they would not have the benefit of protection from the First Amendment.

It should be noted that there would be cases where geographic/jurisdictional boundaries would not always strictly correspond to the nodal community created on CNBUG. This situation might arise in the areas where community borders crossed over and created hybrid 'super communities'. Overlapping jurisdictions often occur in areas that share fundamentally the same values, for example, northern New Jersey as a part of New York City (although New Jersey and New York State have different state laws), or the overlap between Switzerland and France in the vicinity of Geneva (both countries have different federal laws). The existence of a hybrid super community would not necessarily destroy the effectiveness of the proposed CNBUG Model, even if the legal systems were, different. For example, there is cooperation between New York and New Jersey, such that a criminal who crossed state lines would not be immune from prosecution. Normative enforcement would unlikely be affected by a hybrid 'super community' because super communities are often based on areas that share similar community norms.

CNBUG versus the Peer Production Model

Unlike the first two models, Peer Production relies on decentralized Internet governance by placing full responsibility and accountability on the individual user. Decentralization presents many advantages over a centralized government, such as not having an overseeing body in charge of making decisions for all users, eliminating over-inclusive or under-inclusive regulation of speech, and settling concerns regarding accountability. Because Peer Production users can decide whether they allow a communication to go through, they are fully accountable for their exposure to online

---

[47] nyc.newyork.NODE (see also part two of this article).

communications. Finally, since Peer Production does not rely on the bureaucratic decision-making practices of a central authority, it allows users to block online threats as soon as they appear.

Despite its strengths, Peer Production's successful implementation depends on a fundamental change in the Internet's structure because it relies on the creation of a trust-based global communication infrastructure. Allowing or disallowing communications to flow according to whether the communicating user is trustworthy is flawed for two reasons. First, because establishing trust online is challenging and never one hundred percent foolproof; and second, because limiting exposure to communications based on trust has the potential to create online isolation.

The Accountable Internet's authors have conceded that the required widespread adoption of authentication (trust) would necessitate 'a major state change' for the Internet that could amount to the 'addition of a new social layer to the Internet protocol stack'. Such a significant change would somehow be based on the Internet users selecting software code 'that reliably serves our social values' (presumably defined globally, democratically, and within a reasonable time frame). Conversely, a successful implementation of CNBUG would not require changes to the Internet's architecture; this system of online governance could be enabled to function with minimal disruption to the existing infrastructure. One means of implementing CNBUG would be by creating a 'dot node' (.NODE), a new online community space via top-level domain[48].

Governance accountability depends on trusting the system. Trust is even more important in a decentralized governance model than in a centralized governance model because in the latter model the users always know who is ultimately accountable. To function effectively, Peer Production requires a high degree of accountability, which would be impossible to establish without a trustworthy online voting mechanism. According to the Accountable Internet's authors[5], new "...technologies will enable both end users and access providers to accept messages and establish connections based on trust in the originating

---

[48] See part 2 of this article for a suggested CNBUG implementation.

party." *Trust* in their article has been defined as "…the ability to decide with whom to communicate" (i.e., as a *two-party decision process*), rather than the more conventional Internet definition of trusted systems as "…centralized means of administering permissions for access to particular documents", which they also cite in the same article. In very large transactional systems like the Internet, a two-party decision process is unreliable. E-commerce experience[49][50] stresses that three-party trust is much stronger, especially where the third party is a neutral and reputable third-party certifier. Additionally, "In an environment where third parties are omnipresent and technologically required, their effect becomes a dominant factor in the dynamic accountability equilibrium[51]."

In effect, the CNBUG architecture (implemented via a .NODE top-level domain) acts as a third party certifier, and in addition, distributes the responsibility of third party certification among numerous actors rather than relying on two parties. It is possible to distribute the responsibilities of a third-party certifier among more than three parties, and still achieve adequate levels of trust[52]. Governance based on two-party trust or authentication would not serve as an effective means of reducing the amount of bad actors online.

In addition to problems related to online security, limiting interaction to certain 'authenticated' or 'trusted' users creates the potential for online self-isolation. As in real life, the majority of Internet users are 'good actors' and, therefore, online isolation effectively stifles one of the Internet's principal benefits: the interconnection of strangers and new ideas. Instead of opening themselves to boundless communications with

---

[49] S. Srinivasan, *Role of Trust in E-Business Success*, Information Management & Computer Security, Vol. 12, No. 1, 66-72, 2004.

[50] Canzaroli, A., Tan, Y.H. and Thoen, W. *The Social And Institutional Context Of Trust In E-Commerce", Proceedings Of Autonomous Agents*, 65-66, 1999 Workshop on Deception, Fraud and Trust in Agent Societies, (1999).

[51] Nimrod Kozlovski, *Designing Accountable Online Policing*, http://islandia.law.yale.edu/isp/digital%20cops/papers/kozlovski_paper.pdf (last visited, August 10, 2006).

[52] Judith Stafford and Kurt Wallnau, *Is Third Party Certification Necessary?* In Proceedings of the 4th ICSE Workshop on Component-Based Software Engineering, Toronto, Canada, May 2001.

seemingly infinite users, users would effectively shut themselves off to most online strangers.

The main reason why CNBUG is a more effective means of centralized governance than Peer Production is because instead of punishing the actor by blacklisting, CNBUG only 'punishes' the act itself, by allowing for the removal of the individual posting. CNBUG participants do not govern the Internet by banning users; instead they govern by banning individual postings that do not comply with their community's norms. By dealing with the credibility of the posting rather than credibility of the person who created the posting, CNBUG does not rely on trusting either governments or private enterprises to govern the Internet, a concern raised by critics of an early version of the Accountable Internet[53]. This governance concept embodies three principal benefits: it allows for the preservation of online anonymity, it permits a good actor who committed a bad act to rectify the problem, and it integrates accountability into each removal decision in the form of quorum flagging.

CNBUG's flagging system allows for the preservation of online anonymity, which is an important means of disseminating speech protected under the First Amendment[54]. A good actor, for example, might want to retain their anonymity (perhaps for political purposes in places like China or Iran) and refuse to go through a verification system or self-tagging. Communication with such unidentified users in Peer Production would be barred, because they would not have established 'trust' and there would be no means for them to appeal their status ("Hey, I'm not bad, I just want to remain anonymous"). Even if they were to become a part of a trusted network, trusting an anonymous user undermines the fundamental character of any trust-based system. CNBUG allows for anonymity because it substitutes Peer Production's trust 'tagging' concept with consensus 'flagging', which means that users do not need to identify themselves in order to communicate. On CNBUG, communications can be removed, but not the speakers themselves.

---

[53] Susan Crawford blog *The Theory of Everything* http://scrawford.blogware.com/blog/_archives/2004/2/6/18830.html posted February 6, 2004 (last visited, August 10, 2006).

By allowing for the removal of communications instead of the banning of users, CNBUG effectively creates an integrated rectification mechanism. In Peer Production, if a good actor made a bad judgment and was resultantly banned (for example by forwarding a link to a "Free Ipod Referral" that they genuinely believed to be legitimate), by virtue of being banned, they would be unable to appeal their status. Conversely, on CNBUG, the offending post would be flagged and then removed, and the poster would be automatically notified via email that their post was removed and which of the flags[55] triggered its removal.

This form of notice allows inadvertent bad actors to modify their behavior, thus avoiding future removals. As it stands under Peer Production, once a user is blocked/blacklisted, it would be difficult for them to remedy the issue and re-integrate themselves to the online community. The Accountable Internet's authors have acknowledged the risk of overreaction and collateral damage from 'guilt by association' and through 'the power of banishment' as potentially the most undemocratic characteristics of Peer Production[5].

Finally, CNBUG integrates decisional accountability by requiring a quorum to meet a flagging threshold prior to removing a post from the system. Removal by quorum minimizes the danger of overzealous enforcement, especially when technological safeguards are integrated to ensure that users are not flagging maliciously. CNBUG's flagging system would work without human review, with the offending post automatically deleted as soon as the pre-defined flagging threshold were reached. The flagging threshold would be dynamically set by a basic algorithm that calculated the threshold value according to

---

[54] *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995) (The Supreme Court applied exacting scrutiny to determine that anonymity in political speech is a specially protected right under the First Amendment).
[55] As defined below, on Craigslist there are four different flags that may have triggered a posts removal. The threshold must have been met for but ONE of the four flags. Meeting the required threshold across several flags (i.e. if it is flagged as spam and also prohibited, but there are insufficient flags to satisfy the threshold for one or the other), then the post is not removed. In this case, I expect that CNBUG would encompass the four basic Craigslist flags (miscategorized, prohibited, spam, discussion), as well as some new ones (i.e., Intellectual Property or notify local police).

objective[56] inputs, such as the volume of posts in the category/site, frequency of visits, frequency of new posts, and the 'volatility' of the category (e.g., sexual encounters would be more volatile than lost pets[57]).

On the whole, CNBUG overcomes the problems posed by Peer Production's outright banning of noncompliant participants while preserving the Internet's open communications character and fundamental architecture.

Disadvantages of the CNBUG Model

Despite having many benefits over the previous three models, CNBUG encompasses certain weaknesses. One of its residual disadvantages is that despite a CNBUG node being organized as a decentralized peer-governed entity, there must still be an overseeing body to determine the community node's terms of use and to re-examine removal decisions challenged by the post originators. Having a governance board make these decisions might revive some of the problems prevalent in Benevolent Dictator and Democracy. However, unlike in the other models, local representatives elected to oversee a node under CNBUG would have a better understanding of their own community's norms and values, and can still be held democratically accountable to their community.

Another limitation of CNBUG is that, at least initially, it would be difficult to implement it on an Internet-wide basis. Since the model's main advantage stems from dividing the Internet into geographical locations[58], multinational corporations (such as Amazon or eBay) that might like to have a presence on each community node would have to comport with each node's community standards. Under the CNBUG model, this can be achieved by having each individual Web site integrating itself into the flagging system and allowing themselves to be governed (See CNBUG article 2, implementation).

---

[56] The term 'objective' signifies here that the input values could be determined according to the system's normal usage statistics, rather than by a single person or entity. For example, if there are 100 posts in a particular category determined at a certain time of day, i.e., in a non-volatile category with 10 new posts daily, the algorithm would compute a threshold value that when triggered (say by 5 flags) would remove a post in that category when the threshold was met. From a comment on the first draft, courtesy of Prof. Susan Crawford.
[57] An appropriate analyst would determine the actual flagging variables and the algorithm itself could be adjusted if it were found ineffective.
[58] Or, if applicable, to a professional association, etc.

Despite overcoming the danger of individual user isolation on Peer Production, CNBUG might create certain level of nodal city/state/country isolation. Encouraging users to center their Internet experience locally rather than globally might curb the Internet's objective of global interaction[59]. A practical way to offset this problem is to have the CNBUG nodal system exist as a subset of the 'regular' Internet, meaning that users participating in their own community node would be subject to all its rules and safeguards, but would not necessarily have the same expectations when leaving the node to surf the open Web.

Finally, CNBUG would have to diligently safeguard against those users that would form an 'angry online mob' that could collectively fulfill the flagging threshold requirements of posts that they disagreed with, thus censoring community speech that was not actually violating its normative standards. As noted above, this problem could likely be remedied with an arsenal of sophisticated technological safeguards that limit the amount an individual user can flag in a day and also allow for review of appealed removal decisions.

Conclusion

By evolving and modifying the beneficial aspects of Peer Production, CNBUG manages to create a viable alternative to governing the Internet that resolves many outstanding issues present in the three other models of Internet governance. Phase 2 of this article proposes a practical implementation of the CNBUG concepts.

Acknowledgements

---

[59] This issue may not be as prevalent on a professional organization whose rules and regulations are less dependent on geography.

Appendix A: A Brief Introduction to Craigslist.org

In 1995 Craig Newmark observed virtual communities of Internet users helping each other out on various Web sites and newsgroups. He decided to join the cause and created a Web site whose initial purpose was to inform people about events in San Francisco, California. The site became popular by word of mouth and eventually required a devoted server. Newmark wanted to call it "San Francisco Events" but his friends urged him to name it 'Craigslist', reflecting the site's personal and down-to-earth nature. Newmark wrote code that enabled users to automatically add postings, evolving the site into craigslist.org ("Craigslist").

The current version of Craigslist is a simple, text-only interface that serves as an enormous global classifieds hub composed of cities and states, spanning six continents (See *Figure 1*). Craigslist's popularity grows every day and is due entirely to word of mouth.[60] It has become a global online phenomenon, changing cities, impacting newspapers, and at one point ranking as the seventh most visited site on the Internet.[61][62]

How Craigslist Works

On Craigslist, users have the ability to browse ads, search the system, post in discussion forums, and contact other users. By and large users conduct their searches and postings in the city where they live or work. Some of the cities are themselves divided up into smaller regions. New York City, for example, is subdivided into the five boroughs (Manhattan, Brooklyn, Queens, Bronx, Staten Island), but its Craigslist's community also includes upstate New York, Long Island, and even nearby areas of Northern New Jersey. Similarly, Switzerland's Geneva Craigslist community includes the adjacent region of France.

To post a listing on the system, users must select their community area ("node") and from their node's main page, choose the category corresponding to their posting and click the 'post' button. If they have an account and are logged in at the time, the listing is

---

[60] Philip Weiss, New York Magazine, The Rise of Craigslist and How It's Killing Your Newspaper, January 31, 2006.
[61] http://www.craigslist.org/about/pr/factsheet.html
[62] Philip Weiss, New York Magazine, The Rise of Craigslist and How It's Killing Your Newspaper, January 31, 2006.

immediately posted. Otherwise, the users are emailed a confirmation notice that they must activate by clicking on a link and selecting 'publish' before the listing is posted to the site. A posting on Craigslist can be made whether or not a participant is a member, which lowers the threshold for participation. In addition, users have the option to use their real email address or an 'anonymized' address[63], or even have the option to include a phone number but no email.

Essentially, Craigslist functions as a simple to use, convenient and free online town square where users interact with each others in their local community.

The Craigslist's Method Post Removal: Flagging

On a monthly basis, users from around the globe post approximately 10 million classified ads and 40 million discussion postings[64]. Craigslist, however, has only 19 employees, making any kind of staff content review and moderation unfeasible. Instead of relying on its employees to govern the site, Craigslist has implemented a flagging system that allows all users (participants) to act as moderators. At the top of each Craigslist posting are five flag buttons; four of which remove the listing from the system and one that nominates it for the 'best of' Craigslist (See *Figure 2*).

- If a listing is flagged as *miscategorized*, it means that it was posted in the incorrect category, such as posting a watch for sale in 'cars and trucks'.

- *Prohibited* includes items that are not allowed to be sold, as well as any kind of improper (libelous, invasive, abusive, harassing, etc.) statements, misrepresentations, deception, infringement, legal violations, or posts that are a violation of netiquette (such as viruses or attacks).

- The *spam* button is for flagging multiple posts advertising the same item in different categories, links to eBay auctions, pyramid schemes, chain letters, and links to online businesses for which there is a separate category.

---

[63] Craigslist gives the option to anonymize an email address, which creates a random address such as anon-22222@craigslist.org to avoid spam.
[64] http://www.craigslist.org/about/pr/factsheet.html

- The *discussion* button flags posts that comment on other posts, such as if something is a scam, or someone posts an argument regarding a seller or an item's price.

- The final *'best of'* button is the only one with positive connotations and is used to indicate a funny, entertaining, well-written, or well-liked post. *'Best of'* is the only category that is reviewed by staffers after being flagged to ensure that it is truly deserving of inclusion in this category.

For a post to be deleted, it must receive a certain amount of flags. The flagging threshold that triggers post's deletion is determined by the Craigslist staff, and varies according to city and category, with the exact threshold value kept secret.
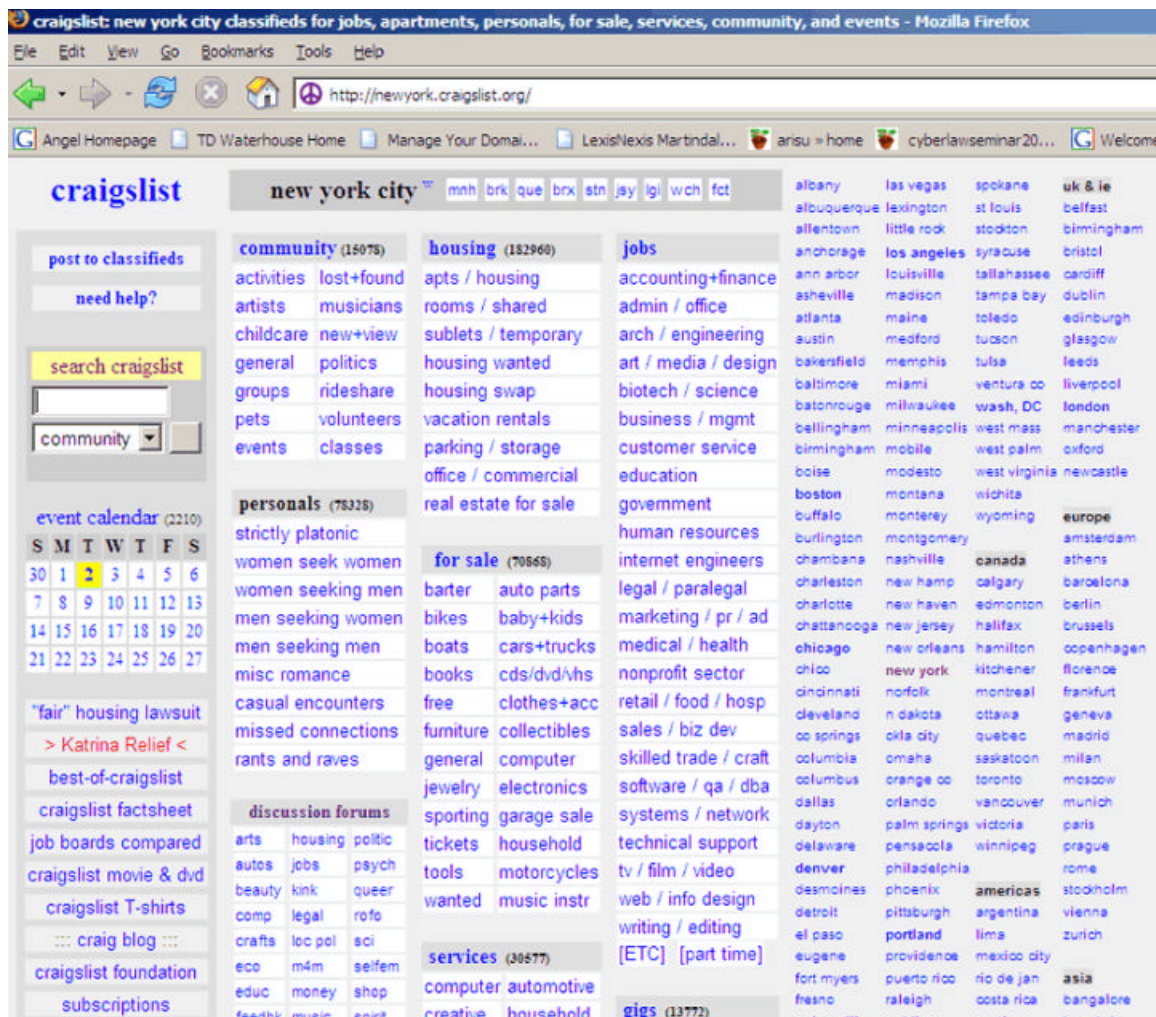

Figure 1: Screenshot of Craigslist New York City Main Page

please flag with care : [miscategorized] [prohibited] [spam] [discussion] [best of]

email this posting to a friend

Figure 2: Screenshot of Craigslist's Five Flags

thanks for flagging!

- If you flagged by mistake, don't worry -- it takes more than one flag to affect a posting.

- Approximately 5% of all craigslist postings are removed through community flagging.

- 98% of postings removed by flagging are in violation of the craigslist terms of use.

On behalf of craigslist and the entire free world, thanks for taking the time to flag!

Continue browsing free stuff on new york craigslist

(Please share your suggestions for improvement in our feedback forum)

Figure 3: Post flagging notice: Removal statistics

Appendix B: Principal Advantages/Disadvantages of Different Internet Governance Models

Table 1

Principal Advantages/Disadvantages of Different Internet Governance Models

#	Principal Characteristics of Internet Governance Models	Benevolent Dictatorship	Democracy	Peer Production	Craigslist (Local Information and Classified Service)	CNBUG
1.	**Governance**	Centralized non-democratic	Centralized democratic	Decentralized	Decentralized, but with centralized non-democratic aspects	Decentralized democratic
2.	**Service Administration Method**	Appointed by the dictator	Democratically elected	Self governed by user	Appointed by the company	Self governed
3.	**Method of individual record's removal**	Notification sent to the 'dictator' who ultimately makes and enforces decisions. Dictator determines compliance according to guidelines or even by arbitrarily changing guidelines time to time or in response to the external pressure (i.e., from the media).	Notification sent to the government body, which makes the decision of compliance according to democratically determined guidelines	Blacklisting from self-selection process	Triggered upon flagging threshold. Some most important decisions made by the central body	Triggered upon flagging, violations determined by 'community norms', as defined by the quorum majority within a predefined time frame, or by a similar time-sensitive peer/quorum decision mechanism

4.	**Number of people typically involved in an individual post's removal**	Typically 1 (Administrator appointed by the dictator)

The number of people necessary to make a removal decision is static | Typically 1 (Administrator appointed by the board)

The number of people necessary to make a removal decision is static | Typically 1 (The user self-administers)

The number of people necessary to make a removal decision is static | The exact number of flags required to remove a post is kept secret (i.e. 6 flags), and varies depending on the category.

Flag threshold number is determined by a Craigslist administrator

The number of people necessary to make a removal decision is dynamic (it varies depending on the category and other factors) | The exact number of flags required to remove a post is kept secret (i.e. 6 flags), and varies depending on the category.

Flag threshold number is determined algorithmically

The number of people necessary to make a removal decision is dynamic (it varies depending on the category and other factors) |
5.	**Notification of an individual post's removal**	Dictator sometimes notifies but there is no obligation to do so	Administrator sometimes notifies but there is no obligation to do so	No notification	System automatically sends notification email to violator	System automatically sends notification email to violator
6.	**Sanctions upon violation**	Varies from warning to banning from system	Varies from warning to banning from system	Inability to interact with this particular user	Warning, no banning from system	Warning, no banning from system
7.	**Legal Enforcement**	Dealt with according to internal policies, then authorities are contacted if necessary	Legal action might be deferred to territorial enforcement authorities	User must contact the authorities to trigger legal enforcement	Territorial enforcement authorities can prosecute/enforce independently without notification to system administrator	Territorial enforcement authorities can prosecute/enforce independently without notification to system administrator
8.	**Governing rules**	Policy statements of the company set by the company's attorneys	Set by the democratically elected body, likely in conjunction with or deference to existing legal territorial regimes	The user has full discretion	Basic terms of use set by the system administrator. American Constitution-like in its simplicity and open to interpretation. General moral and legal principles	Basic rules set up for each geographic or professional node based on existing laws. Additionally governed by the community's norms

9.	**Checks and balances**	None, private corporation makes its own rules, users have the option of not participating. Open market competitors might exist.	Democratic voting system	None, users has have absolute control over their online destiny participation or openness to the peers	A removal decision must be okayed by a pre-set threshold of independent users based on the guidelines defined by the Service Owner	A removal decision must be okayed by a pre-set quorum/threshold of independent users based on the democratically defined guidelines
10.	**Responsibility to govern**	Depends solely on the dictator	Depends solely on the democratically defined service governing charter and elected governing body	Depends solely on the user	Depends solely on the Service Owner's voluntary delegation of most (but not all) responsibilities to the entire nodal community + the overseer	Depends solely on the involvement in a particular class of the transactions of the entire nodal community or geographically /professionally defined sub-segment quorums of the global community
11.	**Speed of response to threats**	Slow, relies on bureaucracy	Slow, relies on bureaucracy	Instant	Can be very fast, depending on the egregiousness of the violation. Relies on a quorum. Users might act faster if they perceive an injustice	Can be very fast, depending on the egregiousness of the violation. Relies on a quorum. Users might act faster if they perceive an injustice
12.	**Acceptance of anonymity**	Accepted, but the underlying information is always known. Can be subjected to disclosure according to law or even corporate policy	Unknown	Unlikely to accept	Accepted, but can be tracked down by the territorial enforcement authorities if absolutely necessary. To ascertain identity is difficult but not impossible	Accepted, but can be tracked down by the territorial enforcement authorities if absolutely necessary. To ascertain identity is difficult but not impossible
13.	**Liability for defamatory content**	None according to the CDA safe harbor provisions (*Zeran v. AOL*)	None	Inapplicable	None	None

| 14. | Main weaknesses | • Users interests are completely up to the dictator's discretion

• Users have no power

• Bad reputation for customer service | • Impossible to establish a set of uniform global Internet rules due to enormous variations in world-wide community standards

• Potential imbalance of representation due to the digital divide

• Difficulties in enforcement of democratic Internet governance rulings by some territorial governments | • 'Reverse-chilling' effect, overly broad blocking or filtering criteria prevent users from some content

• Prevents the interconnection of strangers

• Restricting the participation of new users

• A bad actor can pretend to be a good actor up until a certain point, as there is no way to ascertain character forever

• Changes the basic architecture of the Internet | Inapplicable | • There must still be an overseeing body to determine the community's terms of use and review challenged removal decisions

• Initially unfeasible to implement on an Internet-wide basis; a global service provider would have to comport with each geographic node's norms and laws

• Requires safeguards against users that could form an 'angry online mob' that might censor speech in their community by fulfilling the flagging threshold |