GigaNet Sixth Annual Symposium, Nairobi, Kenya 26 September 2011

Upholding online anonymity in Internet governance: Affordances, ethical frameworks, and regulatory practices

Robert Bodle, PhD, College of Mount St. Joseph, USA

Abstract

This paper argues that anonymity in networked digital communications is indispensable as an enabler of other inalienable rights, including informational privacy and freedom of expression. This work traces how an alignment of government policy and private interests, norms, practices, and ethics assert a persistent identity ecosystem online. And it reappraises the democratic uses, techno-social affordances, and human rights dimensions of online anonymity to help shape discourse that can guide policy makers and other stake-holders towards its protection.

Introduction

Online anonymity is increasingly at risk of becoming extinct. A rash of defamation lawsuits have eroded legal protection for anonymous defendants (Kerr, Steeves, & Luckock, 2009). Intellectual property maximalists want to track and monitor infringing uses/users (Washing Declaration on Intellectual Property and Public Interest, 2011). Nation-states and heads of state claiming national security want to monitor citizens' online communication and increase data retention (e.g., France, Germany, South Korea). Law enforcement agencies want to lower the legal threshold to use information technology to track and convict criminals (e.g., GPS-enabled ubiquitous surveillance). And a powerful ad-funded Internet industry is collectively advocating for real name only policies, while creating an online environment that prevents anonymous participation by design. These combined factors suggest a climate increasingly hostile to anonymity and pseudonymity in networked digital communications. Adding to this climate is the unprecedented technological ability to track people online.

On April 10th, 2010, at its annual developer event, Facebook introduced Open Graph, including the social plugin, the "Like" button, which capped five years of interoperable features that enable users to tie their Facebook identities to external sites, applications, and devices (Bodle, 2011). More recently, in June 2011, Facebook implemented face-recognition technology that attempts to match users' friends' faces with their names (Rosen, 2011). Technically, now, it is incredibly easy to maintain a persistent user identity on the Web. In fact, it is becoming the default by design. Enhanced tracking capabilities help companies and governments identify and track people online and offline via social plugins, HTTP cookies, search engines, browsers, operating systems, wireless networks, cloud services, SNSs, Open APIs, apps, devices, Global Positioning Systems, Internet and mobile service providers, and other intermediaries. Added to this technical means is a strong market incentive to promote fixed user identity.

With technological means (interoperability), product design (opt-out defaults), and market incentive, Facebook reinforces social norms and attitudes that favor a persistent identity ecosystem, leading one industry analyst to concede, "Essentially, we are moving beyond the point of no return" (Solis, 2010). In pursuit of Facebook is Google with its burgeoning social network Google+ that also blocks the accounts of people who use pseudonyms instead of their real names (Rosenbach & Schmidt, 2011; Kirkpatrick, 2011). Persistent user identity is quickly becoming the norm on other major online portals, social network sites (SNSs), news sites, blogs, and forums (and across devices). Moreover, several countries, empowered by technology companies, "have established a real-name identification system before users can post comments or upload content online" (La Rue, 2011, p. 15).

There is growing interest in government and in the entertainment industry to track users online in order to protect intellectual property (IP), reflected in proposed trade agreements (e.g., ACTA) and legislation (e.g., PROTECT IP) that would require the help of Internet intermediaries to "assist governments and others who seek to discover the identity of anonymous authors" (Froomkin, 2009, p. 443). Intermediary liability is one form of censorship, under the guise of national security (York, 2011). This collusion between governments and IP holders, suggests Mueller, reflects a "convergence between the systematic surveillance practices proposed by would-be enforcers of IP protection and those utilized or proposed by the national security state" (2010, p. 156). National security and business interests, together, are prioritizing the protection of intellectual property, tilting the balance against Internet freedom, resulting in "a disproportionate violation of citizen's rights to communication" (MacKinnon, 2011).

Although it may seem that anonymous speech on the Internet "has to go away," as some have suggested (Bosker, 2011), anonymity enables fundamental freedoms and rights online, and without its protection, privacy and freedom of expression are also at risk. These rights are enshrined in constitutions, recognized in the Universal Declaration of Human Rights (UDHR, 1948) and the International Covenant on Civil and Political Rights (ICCPR, 1967, 1976), enforced, though unevenly, in international law and policy, and acknowledged as protecting the extrinsic good of liberty, political freedom, self-determination, autonomy, dignity, power, and the ability to think and speak without censorship or surveillance (Ermert 2009; Hosein 2006; Tavani 2011; La Rue 2011). In order to have a "people-centred, inclusive and development-oriented Information Society" (WSIS, 2003), we need to protect these rights, including anonymity, or they will "go away" (Bosker, 2011).

The ability to speak anonymously has traditionally been understood as enabling broader democratic rights in the US Constitution and Supreme Court (McIntyre v. Ohio Elections Commission 1995), and interpreted in the digital age by the Council of Europes' Declaration on Freedom of Communication on the Internet (2003). In a new report to the UN General Assembly, Frank La Rue (2011), Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, writes "Indeed, throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously" (p. 15). "Anonymity," Hosein asserts, "is key to public participation and the functioning of an open and participatory democracy" (2006, p. 131). Moreover, it is essential

for voters, political dissidents, and corporate whistleblowers to communicate without repercussion or retribution (2006, p. 131). Anonymity online also protects people from violence offline, including sexual abuse victims and other vulnerable and marginalized populations.

Social network sites have become major platforms for pro-democracy activists and journalists who use pseudonyms to protect themselves from repressive regimes. Facebook, through its culture of persistent ID and real name only policy, has rendered civic actors who use the network "vulnerable to government spying" (Durbin, 2011). It is evident why human rights supporters and civil society groups condemn real name only policies in popular online spheres (Fay, 2011; Pfanner, 2011; York, 2011). The loss of anonymity and pseudonymity in online spaces has a chilling effect on freedom of expression and undermines privacy. Yet, there is a pronounced lack of consensus about whether online anonymity, which supports these other rights, should also be protected. By looking at leading research into the affordances of anonymous interactions, underlying ethical frameworks, and existing governance practices, I hope to contribute to a greater understanding of why online anonymity should be upheld as a right and maintained as an integral component of a human rights policy agenda in Internet Governance and beyond.

Methodological Background

Online anonymity is often difficult to defend because by removing attribution or accountability, immoral and criminal activity can be encouraged (Plato's Gyges' Ring or "the immoralist's challenge;" Kerr, Steeves, & Lucock, 2009, p. xxiv). Criminal abuses suggest that anonymity is not an absolute right, however disproportionate responses to potential harms often obscure the benefits. To fully appreciate the value of online anonymity and why it should be protected, I draw on insights from leading studies in communication, media studies, and sociology of its uses and affordances by individuals and groups (e.g., minimal accountability, disinhibition and deindividuation). These findings dispel some of the myths that fuel moral panic over anonymous online communication by illuminating the multiple effects of anonymous interactions.

The rift between competing views of anonymity and persistent user identity exists at many levels, including the level of culture, rhetoric, public policy, technological design and use, and ethics. I explore the ethical justification for these competing views and formulate a pluralistic approach that combines the social utility framework with a Categorical Imperative, rights-based view that recognizes anonymity as an important enabler of other existing rights, "an instrumental good" (Spinello, 2003, p. 75) and worth protecting. I suggest how this pluralistic framework can inform the application of proportionality used in regulating a balance of conflicting rights in a multi-stakeholder context. Indeed, comparative ethics can provide insight into balancing the present imbalance of rights and interests of private stakeholders, governments, law enforcement, and civil society.

To articulate regulatory norms, practices, and attitudes regarding online anonymity, I cite

market analysis, industry press sources, terms of service agreements, and public comments by major industry players and heads of state. A survey of existing and proposed trade agreements, censorship laws, and legislation (primarily from the United States and Europe) provides a regulatory context in which to identify conflicts of interests between stake-holders (governments, private actors, and civil society). Points of conflict help identify points of resistance, recommendations for alternatives, and correlative duties for stakeholders (including designers, citizens, policy makers, and companies).

A political economy approach is used to question the intentions of major portals that maintain a persistent user ID, and to further evaluate the conflict of interest between market logic that benefits from identity tracking and mining user information, and citizens' need for privacy, free expression, and a "safeguard against political oppression" (Hosein, 2006, p. 129). Political Economy looks at the "underlying social relations" between online intermediaries, governments, and individuals, to identify unequal power relationships between them (Greenstein & Esterhuysen, 2006, p. 283). This approach also seeks to counter the market values of dominance and user exploitation by upholding human-centric values, norms and principles proclaimed in the Tunis Agenda (WSIS, 2005).

Empirical analysis helps identify various technical means of online tracking used by social networks, and also points to the correlative means of obscuring and anonymizing one's online communication (Horner, Hawtin, & Puddephatt, 2010). Definitions of online anonymity, including "nonidentifiability by virtue of noncoordinatability of traits" (Wallace, 2008, p. 170), "untraceable anonymity" (Froomkin, 1996), and "unreachability" (Nissenbaum, 1999), help explain ID strategies used by Facebook and others. These strategies do not rely on "merely withholding a name," suggests Nissenbaum (1999), but on preventing "all the crucial bits of information being divulged or inferred" ("opaque identifiers"). It is also important to distinguish between anonymity, privacy, and invisibility, as "the power of the Internet lies not in the ability to hide who we are, but in freeing some of us to expose ourselves and to make ourselves visible on our own terms" (Kerr, Steeves, & Lucock, 2009, p. xxxi).

Affordances, Attributes, and Benefits

The affordance of anonymity online minimizes accountability, encourages disinhibition, and can have depersonalization effects. And while these attributes can make abuses possible, they also provide many benefits for individuals and groups. The rift between those who embrace anonymity and identity multiplicity, and those who distrust it, has existed within virtual online communities and continues to the present. Accounts of early Internet culture on computer bulletin boards, Multi-User Dungeons, and virtual communities depict the embrace of multiple identities for play, experimentation, and raising awareness about social roles (Turkle, 1995). Yet, one of the oldest online community discussion boards, The WELL (Whole Earth 'Lectronic Link), founded by Stewart Brand and Larry Brilliant, explicitly built anonymity out of the community's system design and governance. "One important social rule . . . Nobody is anonymous," wrote Brand, "Everybody is required to attach their real userid to their postings" (Rheingold, 2000, p. 38). The

founders of The WELL feared that with minimal accountability people would be free to insult one another with abandon, and ruin the community (Smith, 2010). But low accountability cuts both ways.

Low accountability of anonymous communication can encourage criminals and terrorists to flout the law with impunity, and they may be tempted to do so with the prospect of minimal risk of accountability for their actions (Plato's Ring of Gyges scenario). On the other hand, low accountability can also encourage the anonymous person to take risks, try things, experiment with new ideas, develop arguments, and express themself freely —and continue to do so because "anonymity masks . . . failure" (Bernstein, Monroy-Hernández, Harry, André, Panovich & Vargas, 2011). Anonymity offers safety from fear of reprisal and ridicule, enabling vulnerable and marginalized groups to "act, transact, and participate . . . without others 'getting' at them" (Nissenbaum, 1999). Safety from public exposure encourages people to reach out for help, advice, and consolation (Baym, 2010). In this context, requiring real names hampers online participation rather than facilitates it.

Disinhibition on message boards, chatrooms, and forums can encourage abusive, vile, and hateful speech, as well as provoke violence against groups and individuals. Abuses through disinhibition leads some to claim that using real names will have a civilizing effect. This is the reason claimed by both Google and Facebook when defending real name only policies. As Marketing Director of Facebook, Rani Zuckerberg postulated "people behave a lot better when they have their real names down" (Bosker, 2011). According to Google, the company requires real names on its SNS, Google+, in order to uphold "community standards" and ensure "a positive experience for everyone" (Google, 2011). The civilizing effect of identity theory was used to justify South Korea's misguided Real Name Verification Law. The law intended to combat offensive speech and required anyone who posted comments and videos on online public forums, to first identify themselves by their unique government issued 13-digit identifier (Rosenbach & Schmundt, 2011). In researching the "civilizing effect" of the identification law, Cho found that "the majority of troublemakers continued to swear without restraint under their real names" (2011). The research also discovered that the longer people are online and the more experienced contributors are, the less they write offensive comments; suggesting that offensive speech is moderated by online experience, not by using real names (ibid).

Disinhibition can also allow people to speak freely, spontaneously, and candidly about things, enabling intimacy. This may lead to "empowered and uninhibited public opinion" (Papacharissi, 2010, p. 122), enabling a more diverse and vibrant democratic culture. And it can encourage honest self-disclosure, which can be liberating, especially for those who are socially anxious, lonely, and stigmatized. For example, many gay teenagers come out online anonymously and find acceptance, "which can give them the confidence to tell their family and peers offline" (Baym, 2010, p. 116). A common misunderstanding is that anonymous online communication encourages people to lie, misrepresent, and deceive. Yet, research finds the opposite to be true, that the Internet's relative anonymity makes people more inclined to disclose honestly (Whitty & Gaving, 2001; Henderson & Gilding, 2004; Quian & Scott, 2007). As Christopher "Moot" Poole, founder of the anonymous image board 4chan, puts it, "anonymity is authenticity" (2011).

Earlier theories to explain the effects of anonymity suggested that in anonymous contexts, such as crowds, people were more likely to behave anti-normatively due to an experience of reduced self-awareness and accountability (e.g., classic deindividuation theory; Zimbardo, 1969). However, more recent studies find that people who are less focused on personal identity markers, are actually more likely to conform to group norms in anonymous contexts. The application of the Social Identity Model of Deindividuation Effects (SIDE) to computer-mediated communication suggests that a reduction of individuation cues can contribute to a strong sense of collective identity (Spears & Lea, 1994), where people experience "more of a sense of we and less a sense of me" (Baym, 2010, p. 114). Deindividuation effects in large anonymous groups have been found to strengthen a shared sense of communal identity and adherence to group norms, critically important for concerted political action (Bernstein, et al, 2011; Coleman, 2011).

In a recent study, "From the Lulz to Collective Action" (2011), Coleman analyzes hacktivist activities attributed to the group name Anonymous, whose targets and actions have grown more politicized, ranging from The Church of Scientology (Operation Chanology), MasterCard, Visa, and PayPal (Operation Payback), Sony Entertainment (Project Sony), the government of Tunisia (OpTunisia) and New York's financial hub (Occupy Wall Street). Coleman finds that anonymity — with its minimal accountability, deindividuation, and disinhibition — contributes to a strong sense of collective identity and action. One participant writes that identification with the anonymous group "allows individuals to be part of something greater. You don't have to fill out a form with your personal information, you aren't being asked to send money, you don't even have to give your name but you do feel like you are actually part of something larger" (ibid). Remarkably, these anonymous campaigns often express themselves offline in coordination with online activities (e.g., temporary website defacement and takedowns, security breeches, social and political media), where people protest in the tradition of non violent direct action and civil disobedience (e.g., sit-ins, occupations).

Anonymous' collective movement has grown out of the online culture of the influential image board, 4chan (http://www.4chan.org/). Participants on 4chan enjoy anonymity and ephemerality, where over 90% of posts are completely anonymous and most discussion threads last a brisk "five seconds on the first page and less than five minutes on the site before expiring" (Bernstein, et al, 2011, p. 1). Unlike The Well, anonymity is explicitly built into the design and governance of the online community. Posts on 4chan are anonymous by default; the window for attribution, if left blank, is automatically assigned "Anonymous" and if pseudonyms are ever used, they can be reused in the very next post (p. 4). Ephemerality results from a combination of high volume of posts and the site's thread expiration practices, suggests Bernstein, et al, (2011, p. 3). Of particular interest is the way in which the boards' affordances shape the culture of the online community, resulting in findings similar to Coleman's (2011): a high level of participation, adherence to group norms, and a strong feeling of collective identity.

The attributes of online anonymity have proven to be important factors in enabling freedom of expression, community building, and collective action. They also support other social benefits such as providing a safe cover for honest, intimate, and open communication, and enabling vulnerable and stigmatized people to seek emotional and information support, including

people with "medical conditions, addiction, and traumas" (Baym, 2010, p. 82). However, the same attributes that promote beneficial outcomes also enable anti-social behavior such as cyberbullying, griefing, and trolling that can originate on sites like 4chan and move to other spaces on the Web. Similarly, although anonymous groups can launch online campaigns that promote pro-democracy efforts, they can also engage in collective actions that incite intolerance, hate, and violence.

The multiple effects of anonymity clearly lend themselves to a Utilitarian ethics that weigh the costs and benefits, positive and negative outcomes, as a means of justification of anonymous online communication, where the results are predictably mixed. However, the Utilitarian approach does not account for the underlying values of anonymity, including "ideals of justice and human rights" (Spinello, 2003, p. 13), and it cannot account for all of the outcomes and consequences affecting groups. Therefore, a more rigorous appraisal of online anonymity must account for its politics (which falls outside the scope of this paper) and for its underlying ethics.

V. Ethical frameworks

Opponents of online anonymity often minimize its value by applying a Utilitarian or consequentialist framework that calculates the potential harms outweigh potential benefits (e.g., the harm of offensive speech outweighs democracy activists' safety from reprisal from repressive countries). Appraisals of online anonymity and pseudonymity are typically viewed through this framework to justify them as both a social good and social harm. For example: "the greatest good is being served here" (Poole, 2011), and "the benefits of real-name culture outweigh the risks" (Axton qut. in Fay, 2011). Yet, we "cannot rely on consequentialism alone when digital media extends the range of our actions" Ess suggests (2009, p. 176). Utilitarian and consequentialist approaches are inadequate and inappropriate frameworks to address dilemmas that have unintended or unforeseen consequences, and when there is an unclear understanding of who will be affected and within what specific timeframe (p. 176). Although the framework cannot account for all of the consequences of fixed user identity and loss of privacy, they can include: loss of livelihood, damage to reputation, political repression, censorship, physical endangerment, and emotional and bodily harm. As Brandeis-Warren (1890) suggests, the loss of privacy, and the related affordance of anonymity can cause, "mental pain and distress, far greater than could be inflicted by mere bodily injury" (Rpt. in Abelson, Ledeen, & Lewis, 2008, p. 63).

The prominence of Utilitarian ethics in privacy debates, according to Tavani, reflects a shift away from a rights-based approach to a Utilitarian cost/benefits analysis (2011, p. 134). I argue elsewhere that this shift to a Utilitarian framework supports a more business friendly, self regulatory approach that directs focus and responsibility away from user rights, and towards the greater good of enhanced communication technology and online services (2011, p.160). In contrast, Kant's Categorical Imperative or deontological approach provides an ethical model that can be used to pursue a set of moral absolutes regardless of the consequences, applied universally and consistently to achieve a resulting social/moral order (MacIntyre, 1966). The Categorical

Imperative view provides ethical support for The Universal Declaration of Human Rights (UDHR; 1948), derived of legal contracts to help determine states' positive obligations and duties to guarantee ideal legal rights. The UDHR also underpins the intentions of the Tunis Agenda to implement existing rights standards on the Internet (2005). These rights include Article 12—freedom from interference and right to privacy, and Article 19—freedom of opinion and expression. The rights-based view must then recognize anonymity as an important enabler of these other fundamental rights (Ermert, 2009; Hosein, 2006; Tavani, 2011; La Rue, 2011), "an instrumental good" (Spinello, 2003, p. 75) and worth protecting.

Applying human rights consistently on the Internet is difficult because they can be interpreted and applied differently throughout the world, which reflects political differences such as open v. closed societies, as well as growing tensions between the interests of stakeholders, including intellectual property (IP) holders, governments, and human rights advocates. Indeed, President Sarkozy reflects these tensions when he suggests that copyrights are more important than human rights (Masnick, 2011). Balancing the property rights of IP holders with human rights including freedom of expression and right to privacy is particularly vexing. Added to the difficulty, human rights can also conflict within themselves (e.g., defamation cases against anonymous defendants). For example, rights that "protect individuals from attacks on their honour" are commonly "located within the same article that protects privacy" (e.g., in UDHR's Article 12, ICCPR's Article 17, and Article 11 in the American Convention; Karanicolas & Mendel, 2011).

UDHRs present universally legitimate standards and values; however, special conditions require that they sometimes are applied differently. When rights conflict, they need to be balanced according to obligations that are conditional not absolute. One criticism of Kant's Categorical Imperative is its inflexibility and inability to "make room for justified and important 'exceptions to the rule'" (Ess, 2009, p. 181). When two laws conflict, offers Ewing (1965, p. 58), it is hard to see how we can rationally decide between them except by considering the goodness or badness of the consequences; "where it is difficult to avoid an appeal to consequences" (Spinello, 2003, p. 19). Principlism, or applying prima facie duties such as autonomy, nonmalfeasance, beneficence, and justice, according to Beachamp & Childress (1994), can provide additional criteria for reconciling competing provisions of international law. Principlism combined with the social utility and rights-based views, can better account for the fact that "different contexts require us to interpret and apply the same norm in sometimes strikingly different ways" (Ess, 2009, p. 191). For example, we can uphold the right of privacy online, while balancing it against competing interests according to special circumstances such as "criminal justice or prevention of crime," with respect to the principles of "necessity and proportionality . . . in compliance with the international human rights framework, with adequate safeguards against abuse" (La Rue, 2011, p. 22).

The application of balancing criteria to conflicting rights and freedoms is not uncommon in international or state law (e.g., Canada's 2010 Ontario defamation case; Geist, 2011). In US defamation case law, for example, Dendrite requirements are applied to explicitly balance First Amendment protections to freedom of speech with plaintiffs' claims of defamation (Levy, 2011).

Unfortunately, government security and IP concerns are presently undermining court oversight and due process of defendant's rights to anonymity in defamation cases in the US (Froomkin, 2009; Masnick, 2011).

The ethical pluralist approach can be used to combine competing and complementary ethical frameworks that are either insufficient or impractical on their own, to help balance and implement conflicting rights. This approach can also be used to build consensus providing deeper insight and justification for the value and necessity of anonymous online communication as it supports other existing rights, including freedom of expression and privacy. This is especially important given that IP maximalists, nation-states, social network sites, and defamation cases are all tilting the balance away from the protection of anonymity and privacy, and towards online surveillance, censorship, data retention, and persistent user ID.

Regulatory Practices: an imbalance

An alliance of nation-states, IP holders, and Internet companies seem to have reached consensus on downgrading the value and necessity of anonymity online. Consensus building is one outcome of Internet governance ("steering not rowing"), where state and non-state actors reinforce norms, rules, principles and practices in order to frame issues and guide policy outcomes through informal and formal channels. A survey of existing and proposed trade agreements, in addition to data retention, surveillance, and censorship legislation (primarily from the United States and Europe) reveal a regulatory context that is increasingly hostile to online anonymity. In the US there is the proposed PROTECT IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 or United States Senate Bill S.96), backed by entertainment and cable lobbies (e.g., MPAA, RIAA, NCTA) but opposed by major Internet companies (e.g., Google, Yahoo!, eBay). The bill would enable the takedown of infringing websites while claiming large swaths of lawful content in its path, suggest critics (Phillips, 2011). The proposed Protecting Children From Pornographers Act (H.R. 1981) would require ISPs to track individual online activity and store it for 18 months, along with a user's name, address, banking information, and IP addresses. The plurilateral Anti-Counterfeiting Trade Agreement (ACTA) seeks to establish an international standard for enforcing intellectual property rights. In spite of the secrecy as it makes its way through global trade bodies, leaks of the agreement have been roundly criticized by civil and privacy rights NGOs for threatening freedom of expression. Examples of existing legislation to monitor infringing uses on the Internet include HADOPI in France and the Digital Economy Act in the UK. If entertainment companies continue make headway in pushing for enhanced monitoring capacities to enforce IP protection, they will succeed in making persistent user ID a default requirement for Internet use.

The above tide of proposed and existing legislation and trade agreements require the collaboration of digital intermediaries, which "encompasses a range of actors, services and platforms operating in digital environments" including Internet service providers (ISPs), domain name registrars, search engines and portals, and social network sites, among many other platforms, systems, and services (OECD, 2010; Horner, et al. pp. 20-21). It may appear, then, that

more intermediaries should differ in their attitudes toward freedom of expression, privacy, data retention, and user identification. Yet, tracking, storing, and maintaining a fix on people's preferences, purchases, and online behavior is highly profitable to the Internet industries.

Social network giant Facebook plays a prominent role in reinforcing norms and attitudes that favor a persistent user ID ecosystem, with strong market incentives to gather information on real entities for advertisers and other third party businesses (Bodle, 2011). The SNS promotes a regime of sharing that encourages self-disclosure and the maintenance of a persistent traceable online identity. Facebook regulates against anonymity and pseudonymity through community design and governance, suspending and deactivating user accounts based on a strict real-name only policy:

1. You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
2. You will not create more than one personal profile.
3. If we disable your account, you will not create another one without our permission. (From "Statement of Rights and Responsibilities;" Facebook, 2011)

Zuckerberg claims, "The days of you having a different image for your work friends or co-workers and for the other people you know are probably coming to an end pretty quickly . . . having two identities for yourself is an example of a lack of integrity" (Cutler, 2010). This is more a prescriptive statement than it is a descriptive one because Facebook plays an active role in shaping an online culture of persistent user ID, rather than being shaped by it as the CEO suggests (Kirkpatrick, 2010). Facebook's regulatory practices together with its tracking features make it increasingly difficult to achieve anonymity, or one's "nonidentifiability by virtue of noncoordinatability of traits" (Wallace, 2008, p.170). The SNS identifies us and coordinates our traits through social plugins, Open APIs, embedded applications, and other interoperability tools in an attempt to make real identification public by default.

Facebook shapes social norms and attitudes about anonymity and pseudonymity for its users, but also within policy circles, increasing its lobbying presence in the United States (Shapiro, 2011) and participating in international forums including the G8 Summit (Wintour, 2011). The policy stakes coincide with high expectations of the affordances of social media for democratic participation, which contributed to the Arab Spring. Yet, the self-regulatory practices within the Internet industry, along with strong government security and IP agendas, provide a powerful front to overturn the balance of human rights protection online as they compete with the rights of capital and the state.

Recommendations, Conclusion

As Lessig writes, "There is no single way that the net has to be; no single architecture that defines the nature of the net" (2006, p. 32). Although the Internet provides the affordance of anonymity, the Internet is no longer anonymous by default, as it once was. Today anonymity must be intentionally built into community spaces online and upheld by cultural norms, ethics, and regulatory practices. Anonymity by design requires identification to be opt in, not public by default. Pseudonyms should be recognized as a security feature, not a security risk or indication

of "lack of integrity." Additional anonymization and security tools are needed, as Nissenbaum warns, anonymity online is not about control over our names as much as it is controlling access to the crucial bits of information or "opaque identifiers," such as a computer's IP address or a geographic location that can render one "reachable" (1999).

Because online communities shape and are shaped by the affordances of online spaces, community design and governance should reflect the rights of the participants, guided by an expansive and nuanced pluralist ethics. When justifying an ethics of anonymity in online communities the Utilitarian scale of costs and benefits should be combined with other frameworks that take into account the underlying values and ideals of anonymity as an indispensible enabler of other rights, including privacy and freedom of expression. Anonymity is part of a larger project to restore informational privacy and self-determination within the networked digital communication space, which includes the right to participate freely, the right not be tracked, the right to access information about oneself, and the right to delete. And these rights should be balanced against the rights of intellectual property holders and intermediaries with respect to the principles of "necessity and proportionality . . . with adequate safeguards against abuse" (La Rue, 2011, p. 22).

The attributes of anonymity, including minimal accountability, disinhibition, and deindividuation, can encourage robust political speech, provide safety from reprisal, permit the freedom to speak freely, and create a strong sense of group identity. Anonymity can serve the multi-stakeholder model of Internet governance well by encouraging the full involvement of all, including marginalized and vulnerable populations, political dissidents, whistleblowers, and other private citizens who wish to participate without surveillance, data retention, repression, or other infringements on personal autonomy, privacy, and freedom of expression. Perhaps to make the Internet Governance Forum governance process more inclusive, the IGF can encourage anonymous participation in its online forums and remote participation hubs.

The proposal of an "expert panel on the promotion and protection of freedom of expression on the Internet to be convened at the 19th Session of the UN's Human Rights Council" (APC, 2011) holds promise for the institutionalization of similar rights, including the right to online anonymity and data protection (Karanicolas & Mendel). With deeper understanding and recognition of the human rights and democratic dimensions, ethics, and attributes of online anonymity, perhaps we can reach a new consensus about its value and necessity to help shape discourse that can guide policy makers and stake-holders towards its implementation and protection. It is up to all stake-holders including community designers, intermediaries, technical communities, governments, educators, and netizens to work together to build a movement that rebalances public and private interests in Internet Governance, to help fulfill our full human potential in Information Society.