THE ETHICS OF ONLINE ANONYMITY OR ZUCKERBERG VS. "MOOT"

Robert Bodle, PhD,

College of Mount St. Joseph, USA

irpbodle@gmail.com

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. Yet, an alignment of industry norms, practices, ethics, and techno-social design asserts a persistent identity ecosystem, making online anonymity more difficult to achieve. This paper reappraises the democratic uses, affordances, and human rights dimensions of online anonymity in order to advance an ethical justification for its protection.

Introduction

Anonymity online is increasingly at risk of becoming extinct due to a host of converging developments. A rash of defamation lawsuits have eroded legal protection for anonymous defendants (Kerr, Steeves, & Luckock, 2009). Intellectual property maximalists push for a legal mandate to track and monitor infringing uses/users through intermediary liability (Washington Declaration on Intellectual Property and Public Interest, 2011). Democratic and totalitarian alike nations-states monitor citizens' online communication and amass big data on citizens. Law enforcement agencies seek 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 advocates for real name only policies that are shaping an online environment that probihibits anonymous, non-identifiable communication by design. These combined factors suggest a climate increasingly hostile to anonymity and pseudonymity in networked digital communications. Added to these developments is an unprecedented technical ability to share and be tracked online.

With a Facebook account it is incredibly easy to maintain a persistent user identity online In fact, it is becoming the default by design. When Facebook introduced Open Graph in 2010, including the social plugin –the "Like" button— it capped five years of interoperable features that enable users to tie their Facebook identities to external sites, applications, and devices (Bodle, 2011a). In 2011 Facebook implemented face-recognition technology that matches users' friends' faces with their names (Rosen, 2011). Today, algorithm-driven personalization filters mine user information to help third parties serve relevant ads to Facebook users and drive Graph Search, Facebook's social search application. Enhanced tracking capabilities also help governments identify and monitor people online and offline via social plugins and networks, HTTP cookies, Open APIs (application programming interfaces), search engines, browsers, operating systems, wireless networks, cloud services, mobile applications and devices, Global Positioning Systems, Internet and mobile service providers, and other intermediaries. Added to the technical means is a strong confluence of market incentives and state security interests that promote fixed

user identity and downgrade the value and necessity of anonymity online.

Internet companies have strong market incentives to reinforce the norms and attitudes that favor persistent user ID, and to gather information on real entities for advertisers and other third party businesses (Bodle, 2011). Facebook, a strong proponent of real-name only culture, promotes a regime of sharing that encourages both self-disclosure and the maintenance of a fixed traceable online identity. Anonymity and pseudonymity are expressly prohibited on the site with Facebook Terms of Use suspending and deactivating accounts based on its 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)

To justify the above, Zuckerberg echoes a nothing to hide argument, "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" (Kirkpatrick rpt. in Cutler, 2010). Such a statement according to Baym, is "fundamentally naive," (Baym, 2010) and "indicates just how privileged Zuckerberg as a wealthy, white, heterosexual male really is — in other words, someone who has nothing to fear from being transparent about his life, and no need to maintain two different identities" (Ingram, 2010). Zuckerberg's statement is more prescriptive than descriptive as Facebook plays an active role in shaping an online culture of persistent user ID, rather than being shaped by it as the CEO suggests (Cutler, 2010).

In pursuit of Facebook Google's social network Google+ blocked the accounts of people who used established pseudonyms instead of their real names, starting the nymwars (Rosenbach & Schmundt, 2011; Cutler, 2011). Persistent user identity is quickly becoming the norm on other major online portals, social network sites (SNSs), news sites, blogs, and online public forums, as well. In fact,, several countries enabled by Western technology companies, "have established a real-name identification system before users can post comments or upload content online" (La Rue, 2011, p. 15). With the technological means (interoperability), product design (opt-out defaults), market incentive (ad revenue) and dominance, the real name only regime of sharing is making it increasingly difficult to be anonymous online, leading one industry analyst to concede, "Essentially, we are moving beyond the point of no return" (Solis, 2010).

A consensus is growing among governments and entertainment companies about the mutual benefits of tracking people online. Proposed trade agreements (e.g., ACTA) and intellectual property legislation (e.g., CISPA) would require Internet intermediaries to "assist governments and others who seek to discover the identity of anonymous authors" (Froomkin, 2009, p. 443). Regulating intermediary liability for the purposes of identifying infringing uses is a form of censorship, suggests York, made under the guise of national security (2011). This collusion between governments and IP holders, according to 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 that together prioritize the protection of intellectual

property over privacy and Internet freedom, threatens to result in "a disproportionate violation of citizen's rights to communication" (MacKinnon, 2011).

Anonymity and Human Rights

Although some suggest that anonymous communication on the Internet "has to go away," (Bosker, 2011), anonymity helps support the fundamental rights of privacy and freedom of expression. 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), and are widely acknowledged to protect the extrinsic good of liberty, political freedom, self-determination, autonomy, dignity, power, and the ability to think and speak without censorship, surveillance, or retribution (Ermert 2009; Hosein 2006; Tavani 2011; La Rue 2011). To help ensure a "people-centred, inclusive and development-oriented Information Society" (WSIS, 2003), these rights, including anonymity, need protection 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 514 U.S. 334; 1995), and interpreted in the digital context by the Council of Europes' Declaration on Freedom of Communication on the Internet (2003). In a 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) and "a shield from the tyranny of the majority" (*McIntyre v. Ohio Elections Commission*, 514 U.S. 334; 1995). It is essential for voters, political dissidents, and corporate whistleblowers to communicate without repercussion or retribution; "a safeguard against political oppression" (Hosein, 2006, p. 129). Online anonymity also protects people from violence offline, including 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" (Cohen, 2011). It is evident, then, 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, undermines privacy, and threatens people's lives. Yet, there is a pronounced lack of consensus about whether online anonymity, which supports other fundamental human rights, should be protected.

Methodology and approach

Online anonymity is often difficult to defend because the absence of attribution and accountability for one's actions can encourage immoral, repulsive, and criminal activity (Plato's Gyges' Ring or "the immoralist's challenge;" Kerr, Steeves, & Lucock, 2009, p. xxiv). These affordances can enable criminal abuses such as child pornography, illegal gambling, and black market human and drug trafficking, which strongly suggest that anonymity is not an absolute right. Yet, a myopic focus on the harms obscures the benefits and lends itself to an overreliance on Utilitarian risk/benefit analysis, which

prevents a more expanded ethical view. Insights from interdisciplinary studies on the manifold uses and affordances of online anonymity by individuals and groups help mitigate some of the myths that fuel moral panic. And these findings combined with a meta-ethical analysis can help provide a fuller appraisal of its value A gulf between competing views of anonymity exists at many levels, including the levels of culture, rhetoric, policy and governance, technological design and use, and ethics. In order to take fuller account of competing ethical and meta-ethical views (including absolutism), I 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. Indeed, comparative ethics can provide insight into regulating a balance of conflicting rights and interests in a multi-stakeholder context (including civil society, private industry, and government) and reconciling them.

A political economy approach is used to evaluate the conflict of interest between market logic that benefits from maintaining a fixed user ID, and the needs of private citizens' for anonymity/privacy, free speech, and safety. 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 for the Information Society (WSIS, 2005).

Defining online anonymity helps explain identification strategies used by Facebook and others, which may include: "nonidentifiability by virtue of noncoordinatability of traits" (Wallace, 2008, p. 170), "untraceable anonymity" (Froomkin, 1996), "unreachability" (Nissenbaum, 1999), "an anonymous action is not linkable to someone's identity [and] two anonymous actions are unlinkable to each other" (Clarke, Gauvin, Adams, 2009). One should 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"). Understanding the technical means by which companies (and governments) track "the crucial bits" also points to the correlative means of obscuring and anonymizing one's online communication (Horner, Hawtin, & Puddephatt, 2010). 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). Before developing an ethical justification for online anonymity as a fundamental human right, I will first look at its affordances.

The Dilemma of Online Anonymity: Affordances, Attributes, and Benefits

The affordances of online anonymity help minimize accountability, encourage disinhibition, and have depersonalization effects. Yet, while these affordances can make abuses possible, they also provide many benefits for individuals and groups. The rift between those who support anonymity and identity multiplicity, and those who oppose it has existed within virtual online communities from the beginning. Turkle's study (1996) of the uses of anonymity on early computer bulletin boards, Multi-User Dungeons, and virtual communities, suggests that identity multiplicity is useful for play, experimentation, and raising awareness about social roles. Yet anonymity was explicitly prohibited in the design and governance of The WELL (Whole Earth 'Lectronic Link), one of the oldest online community discussion boards,

founded by Stewart Brand and Larry Brilliant. "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 WELL'S founders feared that with minimal accountability people would be free to insult one another with abandon, and ruin the community. But low accountability cuts both ways.

With the prospect of minimal risk of accountability for their actions, criminals may be tempted to flout the law with impunity. On the other hand, the lack of accountability can also encourage the anonymous person to take risks, try new things, explore ideas, develop arguments, and express themself freely because "anonymity masks . . . failure," which can build confidence (Bernstein, Monroy-Hernández, Harry, André, Panovich & Vargas, 2011). Anonymity offers safety from fear of getting caught, but it also offers safety from 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 fact, the most vulnerable people are far less safe when identifiable.

Disinhibition enabled by anonymity on message boards, chatrooms, and forums can encourage abusive, vile, and hateful speech, as well as provoke violence against groups and individuals. These abuses lead some to claim that using real names will have a civilizing effect. As Marketing Director of Facebook, Randi 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 ensure "a positive experience for everyone" (Google, 2011). Some argue that anonymity is a cause of incivility, and thus too high a price to pay (Levmore, S. & Nussbaum, M. 2011). Yet the connection between civility and the use of real names is refuted by recent studies on the use of pseudonyms online (Boniel-Nissam & Barak, 2011; Cho, 2011; Disqus, 2012). The civilizing effect of identification theory guided South Korea's disastrous Real Name Verification Law. The law required anyone who posted comments and videos on online public forums (with more than 100,000 visitors a day), to first identify themselves by their unique government issued 13-digit identifier (Rosenbach & Schmundt, 2011). Cho found that although the Real Name Verification Law was intended to combat offensive speech, "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 the contributors are, the less they write offensive comments; suggesting that offensive speech is moderated by online experience, not by using real names (ibid).

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 & Gavin, 2001; Henderson & Gilding, 2004; Quian & Scott, 2007). Anonymity can encourage honest self-disclosure and be a liberating experience, 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). As Christopher "Moot" Poole, founder of the anonymous image board 4chan, puts it, "anonymity is authenticity" (2011). Disinhibition can allow people to speak freely, spontaneously, and candidly about things, enabling intimacy. This may also lead to "empowered and uninhibited public opinion" (Papacharissi, 2010, p. 122), enabling a more diverse and vibrant democratic culture. A study conducted by Disqus, a commenting platform used by newspapers,

blogs, and other websites, found that people using pseudonyms contributed the highest volume and highest quality of comments (2012).

Earlier theories used 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).

Coleman's study of hacktivist campaigns attributed to the group name Anonymous (2011) documents how their targets and actions, exploits and projects 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). The study finds the affordances of anonymity —minimized accountability, disinhibition, and deindividuation — contribute to a strong sense of collective identity and action. One participant of an Anonymous campaign notes 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, Anonymous campaigns are also taken offline in coordination with online activities (e.g., temporary website defacement and takedowns, DDoS attacks, security breeches, videos, graphics, and memes), continuing in the protest tradition of non-violent direct action and civil disobedience (e.g., sit-ins, be-ins, occupations).

Anonymous' collective actions have grown out of the online culture of the influential image board, 4chan. Unlike The Well, anonymity and ephemerality are explicitly built into the design and governance of the online community. On the site 90% of posts are completely anonymous, which is the default attribution for posting to the site. The text window used to designate attribution, if left blank, is automatically assigned "Anonymous" and if pseudonyms are ever used, they can be reused in the very next post (Bernstein, et al, 2011, p. 4). Most discussion threads on 4chan last a brisk "five seconds on the first page and less than five minutes on the site before expiring" (ibid, p. 1). This ephemerality results from a combination of the 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.

These studies of the affordances of online anonymity have found them to be contributing factors

that enable freedom of expression, community building, and collective action. They also provide support for other social benefits such as a shield of protection for honest, intimate, and open communication, which enables vulnerable and stigmatized people to seek emotional and information support, including people with "medical conditions, addiction, and traumas" (Baym, 2010, p. 82). Yet, 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, anonymous groups have the ability to engage in collective actions that incite intolerance, hate, and violence as well as promote pro-democracy efforts, whistleblowing, and user freedom.

The manifold effects of anonymity predictably result in a mixed bag. A Utilitarian ethical framework can weigh the costs and benefits, the positive and negative outcomes, as a means of justification for anonymous online communication. However, the Utilitarian approach does not account for the underlying values of anonymity, including "ideals of justice and human rights" (Spinello, 2003, p. 13). A more rigorous appraisal of online anonymity must take fuller account of the politics (which falls outside the scope of this paper) and meta-ethics of anonymity.

V. Meta-ethical justification and implementation

Opponents of online anonymity minimize its value by applying a Utilitarian or consequentialist framework that calculates that 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 viewed through this framework can justify it as both a social good and a 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, Ess cautions that we "cannot rely on consequentialism alone when digital media extends the range of our actions" (2009, p. 176). Utilitarian and consequentialist approaches, Ess maintains, are inadequate and inappropriate frameworks to address dilemmas that have unintended or unforeseen consequences, and when there is incomplete understanding of who will be affected and within what specific timeframe (p. 176). Although this framework cannot account for all of the outcomes and consequences of fixed user identity and violations of privacy, it can provide an important starting point: loss of livelihood, damage to reputation, political repression, censorship, physical endangerment, and emotional and bodily harm. And the loss of privacy related to the inability to communicate anonymously can cause, as Brandeis-Warren (1890) suggest, "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 (2011, p. 134), reflects a shift away from a rights-based approach to a Utilitarian cost/benefits analysis. This shift to a Utilitarian framework supports a more business friendly, self regulatory rhetoric that directs focus and responsibility away from users' rights, and towards the greater good of enhanced communication technology and beneficial online services (Bodle, 2011b, 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 Universal Declaration of Human Rights (UDHR; 1948), derived of legal contracts to help determine states' positive obligations and duties to guarantee ideal legal

rights universally to all people, is a prime example of this framework. 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 supports the recognition and validation of online 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.

There is great difficulty in applying human rights consistently because they can be interpreted and applied differently throughout the world. This difficulty is reflected in broad ideological differences between open versus closed societies, and is symptomatic of growing tensions between competing and colluding interests of stakeholders (e.g., intellectual property (IP) holders, governments, and human rights advocates). Indeed Sarkozy, as President of France, articulated these tensions when he suggested 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 this difficulty, human rights can also conflict within themselves (e.g., defamation cases against anonymous defendants). For example, legal 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; but special conditions require that they be applied differently in different situations. When rights conflict they can be balanced according to obligations that are conditional not absolute (or monastic). 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 rights and provisions of international law. Principlism in combination with the social utility and rights-based views – ethical pluralism – 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, one 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 uphold the protection of 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, the interests of 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 reconcile competing 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 intellectual property 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.

Conclusion

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 to 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 encourages the full participation of all (not just the privileged), 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. With deeper understanding and recognition of the affordances and ethics, human rights and democratic dimensions of online anonymity, perhaps a new consensus can be reached about its value and necessity.

References

Abelson, H., Ledeen, K., & Lewis, H. (2008) *Blown to Bits: Your Life, Liberty and Happiness After*

the Digital Explosion. Boston: Addison-Wesley.

Baym, N. K. (2010) *Personal Connections in the Digital Age.* Cambridge: Polity Press.

Beachamp T. L., & Childress, J., F. (1994) *Principles of Biomedical Ethics, Fourth Ed*. New York: Oxford University Press.

Bernstein, M.S., Monroy-Hernández, A., Harry, D., André, P., Panovich, K., Vargas, G. (2011). 4chan and /b/: An Analysis of Anonymity and Ephemerality in a Large Online Community. In *Proceedings of the AAAI International Conference on Weblogs and Social Media* (ICWSM '11).

Bodle, R. (2011a). Regimes of sharing: Open APIs, interoperability, and Facebook. *Information, Communication & Society* 14(3), pp. 320-337.

Bodle, R. (2011b). Privacy and Participation in the Cloud: Ethical Implications of Google's Privacy Practices and Public Communications. In K. German, & B.E. Drushel (eds.), *The Ethics of Emerging Media: Information, Social Norms, and New Media Technology*. New York: The Continuum International Publishing Group

Boniel-Nissam, M., & Barak, A. (2011) The Therapeutic Value of Adolescents' Blogging About Social–Emotional Difficulties. *Psychological Services*. (Online) Available at http://www.apa.org/pubs/journals/releases/ser-ofp-boniel-nissim.pdf (accessed October 1, 2012.

Bosker, B. (2011) Facebook's Randi Zuckerberg: 'Anonymity Online Has to Go Away.' *Huffington Post*. (Online) Available at http://www.huffingtonpost.com/2011/07/27/randi- zuckerberg-anonymity-online_n_910892.html (accessed October 10, 2011).

Cho, D. (2011) Real Name Verification Law on the Internet: A Poison or Cure for Privacy. In *Proceedings of the Tenth Workshop on Economics of Information Security* (WEIS, '11). Available at http://weis2011.econinfosec.org/papers/Real%20Name%20Verification%20Law%20on% 20the%20Internet%20-%20A%20Poison%20or%20Cu.pdf (accessed October 10, 2011).

Clarke, J., Gauvin, P., & Adams, C. (2009) Exit node Repudiation for Anonymity Networks. In I. Kerr, C. Lucock, & V. Steeves (eds.) In *Lessons From the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*. Oxford: Oxford University Press, pp. 399- 415.

Coleman, G. (2011) Anonymous: From the Lulz to Collective Action. *The New Significance*. (Online) Available at http://www.thenewsignificance.com/2011/05/09/gabriella-coleman-anonymous-from-the-lulz-to-collective-action/ (accessed October 10, 2011).

Council of Europes (2003) Declaration on Freedom of Communication on the Internet. (Online) Available at https://wcd.coe.int/ViewDoc.jsp?id=37031 (accessed September 10, 2011).

Cutler, K. (2010) Why Mark Zuckerberg needs to come clean about his views on privacy. *Venture Beat.* (Online) http://venturebeat.com/2010/05/13/zuckerberg-privacy/ Available at (accessed Septembert 10, 2011).

Disqus. Pseudonyms drive communities. (Online) Available online at

http://disqus.com/research/pseudonyms/ (accessed October 10, 2012).

Cohen, J. (2011) U. S. Senator Asks Facebook for Anonymity Option. *All Facebook*. (Online) Available at http://allfacebook.com/u-s-senator-asks-facebook-for-anonymity-option_b32334?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A %20allfacebook%20%28Facebook%20Blog%29 (accessed October 10, 2012).

Ess, C. (2009) *Digital media ethics*. Cambridge, Polity Press.

Ermert, M. (2009) Council of Europe: Access to the Internet is a fundamental right. (Online) Available at http://www.ip-watch.org/2009/06/08/council-of-europe-access-to-internet-is- a-fundamental-right/ (accessed June 8, 2011).

Ewing, A. C. (1965) *Ethics*. New York: Free Press.

Facebook (2012) Statement of Rights and Responsibilities. (Online) Available at

https://www.facebook.com/legal/terms (accessed October 10, 2012).

Fay, J. (2011) Facebook's position on real names not negotiable for dissidents. *The Register.* (Online) Available at http://www.theregister.co.uk/2011/02/08/facebook_real_names/ (accessed October 1, 2012).

Froomkin, A. M. (2009) 'Anonymity and the Law in the United States'. In *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. New York, Oxford University Press. University of Miami Legal Studies Research Paper No. 2008-42. [Online] Available at: SSRN: http://ssrn.com/abstract=1309225 (accessed October 10, 2012).

Froomkin, A. M. (1996) Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases. Pittsburgh Journal of Law and Commerce 15: 395. (Online) Available at http://osaka.law.miami.edu/~froomkin/articles/oceanno.htm (accessed October 1, 2011).

Geist, M. (2011) Court grapples with legalities of anonymous online postings. *Toronto Star*. (Online) Available at http://www.thestar.com/business/2011/07/31/geist_court_grapples_with_legalities_of_anonymous_online_postings.html (accessed October 1, 2011).

Google. Community Standards. (Online) Available at http://www.google.com/support/accounts/bin/answer.py?answer=107107 (accessed October 1, 2011).

Greenstein, R. & Esterhuysen, A. (2006) The right to development in the information society. In R. K. Jørgensen (ed.) *Human Rights in the Global Information Society*. MIT Press, Cambridge, MA, pp. 281-302.

Henderson, S. & Gilding, M. (2004). "I've never clicked this much with anyone in my life": trust and hyperpersonal communication in online friendships. *New Media and Society* 6: 487- 506.

Horner, L., Hawtin, D., & Puddephatt, A. (2010) Information and Communication Technologies and

Human Rights. European Parliament. (Online) Available at http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=31731 (accessed September 1, 2011).

Hosein, G. (2006) Privacy as freedom. In R. K. Jørgensen (ed.), *Human Rights in the Global Information Society*. Cambridge, MA: The MIT Press, pp. 121-147.

Ingram, M. (2010) Are Facebook's Views on Privacy Naive and Utopian?. *GigaOM*, [Online] Available at: http://gigaom.com/2010/06/01/facebooks-views-on-privacy-are-naive-and-utopian-prof-says/ (December 10, 2010)

International Covenant on Civil and Political Rights (1976) (Online) Available at http://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en (accessed September 1, 2011).

Karanicolas, M., & Mendel, T. (2011) Commentary on the Charter of Human Rights and Principles for the Internet. (Online) Available at http://www.law-democracy.org/wp-content/uploads/2011/10/Charter-Commentary.pdf (accessed October 5, 2011).

Kerr, I., Lucock, C., & Steeves, V. (eds.) (2009) *Lessons From the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*. Oxford: Oxford University Press.

LaRue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. (Online) Available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf

Lessig, L. (2006) *Code and Other Laws of Cyberspace Version 2.0*. New York: Basic Books.

Levmore, S. & Nussbaum, M. (eds.) (2011). *The Offensive Internet: Speech, Privacy, and Reputation*. Cambridge, MA: Harvard University Press.

Levy, P. A. (2011) Litigating Civil Subpoenas to Identify Anonymous Internet Speakers. *Litigation* 37(3). (Online) Available at http://www.citizen.org/documents/litigating-civil-subpoenas-to-identify-anonymous-internet-apeakers-paul-alan-levy.pdf (accessed September 1, 2011).

MacIntyre, A. (1966) *A Short History of Ethics*. London: Routledge.

MacKinnon, C. (2011). Let's Take Back the Internet. TED. (Online) Available at http://www.ted.com/talks/rebecca_mackinnon_let_s_take_back_the_internet.html (accessed September 1, 2011).

Masnick, M, (2011) Should Anonymity Be Dealt With Differently In Copyright Cases Than In Defamation Cases. *Tech Dirt*. (Online) Available at http://www.techdirt.com/articles/20110906/03133815806/should-anonymity-be-dealt-with-differently-copyright-cases-than-defamation-cases.shtml (accessed October 1, 2011).

McCarthy, C. (2010) Facebook F8: one graph to rule them all. *CNET News.* (Online) Available at http://news.cnet.com/8301-13577_3-20003053-36.html (December 10 2010)

McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995). (Online) Available at http://www.law.cornell.edu/supct/html/93-986.ZO.html (accessed September 1, 2011).

Mueller, M. (2010) *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press.

Nissenbaum, H. (1999) The Meaning of Anonymity in the Information Age. The Information Society 15: 141-144. (Online) Available at http://www.nyu.edu/projects/nissenbaum/paper_anonimity.html (accessed September 1, 2011).

Papacharissi, Z. A. (2010) *A Private Sphere: Democracy in the Digital Age*. Malden, MA: Polity Press.

Pfanner, E. (2011) Naming Names on the Internet. *The New York Times.* (Online) Available at http://www.nytimes.com/2011/09/05/technology/naming-names-on-the-internet.html (accessed September 10, 2011).

Poole, C. (2011) Keynote: Christopher Poole. (Online) Available at http://schedule.sxsw.com/2011/events/event_IAP000001 (accessed September 1, 2011).

Quian, H. & Scott, C. R. (2007) Anonymity and Self-Disclosure on Weblogs. *Journal of Computer-Mediated Communication*, *12*(4). (Online) Available at http://jcmc.indiana.edu/vol12/issue4/qian.html (accessed September 10, 2011).

Rheingold, H. (2000) *The Virtual Community: Homesteading on the Electronic Frontier*. Cambridge, MA: MIT Press.

Rosen, J. (2011) Protect Our Right to Anonymity. *The New York Times*. (Online) Available at www.nytimes.com/**2011**/09/13/.../protect-our-right-to-anonymity.htm *(accessed October 1, 2011).*

Rosenbach, M. & Schmundt, H. (2011). Internet Evolution: The War on Web Anonymity. *Spiegel Online.* (Online) Available at http://www.spiegel.de/international/spiegel/internet- evolution-the-war-on-web-anonymity-a-778138.html (accessed September 1, 2011).

Solis, B. (2010) REPORT: Facebook and the New Age of Privacy. Social Media Today. (Online) Available at http://socialmediatoday.com/briansolis/171604/report-facebook-and-new- age-privacy (accessed September 1, 2011).

Spears, R., & Lea, M. (1994). Panacea or panopticon? The hidden power in computer-mediated communication. *Communication Research*, *21,* 427–459.

Spinello, R. A. (2003) The Future of Intellectual Property. *Ethics and Information Technology* 5 (1):1-16.

Tavani, H. T. (2011) *Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing, Third Ed*. Hoboken, NJ: John Wiley & Sons, Inc.

Turkle, S. (1996) *Life on the Screen: Identity in the Age of the Internet*. New York: Simon and

Schuster.

Universal Declaration of Human Rights, The (UDHR) (1948) [Online] Available at http://www.un.org/en/documents/udhr (accessed September 1, 2011).

Wallace, 2008 Wallace, K.A. (2008) On-line Anonymity. In H. Tavani & K. Himma (eds.) *Handbook on Information and Computer Ethics.* Hoboken, NJ: John Wiley & Sons, Inc., pp. 165-189.

Washington Declaration on Intellectual Property and Public Interest (2011) (Online) Available at http://infojustice.org/washington-declaration (accessed October 1, 2011).

Whitty, M. & Gavin, J. (2001) Age/sex/location: uncovering the social cues in the development of online relationships. *Cyberpsychology and Behavior* 4(5), 623-630).

World Summit on the Information Society (2003) Declaration of Principles. (Online) Available at http://www.itu.int/wsis/docs/geneva/official/dop.html (accessed September 1, 2011).

World Summit on the Information Society (2005) Tunis Agenda for the Information Society. (Online) Available at http://www.itu.int/wsis/docs2/tunis/off/6rev1.html (accessed September 1, 2011).

York, J. (2011) This Week in Internet Censorship: China, India, and Faith-Based. *Electronic Frontier Foundation.* (Online) Available at https://www.eff.org/deeplinks/2011/08/week-internet-censorship-china-india-and-faith (accessed September 1, 2011).

Zimbardo, P. G. (1969). The human choice: Individuation, reason, and order vs. deindividuation, impulse, and chaos. In W. J. Arnold & D. Levine (eds.), *Nebraska Symposium on Motivation*. Lincoln: University of Nebraska Press, pp. 237-307.