The Sledgehammer and the Nut: Toward an Elegant Proposition for Online Governance

Grant Patten

Grant Patten is currently pursuing a Master of Information degree at the University of Toronto's Faculty of Information. He holds a Bachelor of Fine Arts degree in Image Arts from Ryerson University. He wrote "The Sledgehammer and the Nut: Toward an Elegant Proposition for Online Governance" for the class INF 1001 Knowledge and Information in Society in the fall of 2009. His website can be viewed at www.grpatten.com. g.patten@utoronto.ca

Steve Jobs, with his iPhone, used a sledgehammer to crack a nut. The iPhone may be seen as a rather heavy-handed solution to the problem of network openness. In an entirely open network, security concerns arise as users have few or no regulations imposed on them for how to interact and exchange information over the network. As a completely tethered appliance, the iPhone is incapable of generating the kind of free-wielding innovation and creativity that the PC environment has long cultivated (Zittrain, 2007). This "appliancized" (Zittrain, 2006, p. 44) approach represents one extreme side of the issue, the other extreme being the "uncompromising end-to-end neutrality" approach (p. 2). This paper shall argue that what is required in order to maintain network generativity whilst ensuring adequate security (Zittrain, 2007) is not an adoption of one extreme over the other, but rather an elegant reconciliation of these two extremes.

For clarification, the terms used above will be defined. The iPhone is a completely tethered appliance because it is essentially welded to Apple in such a way that creative buyers of the product cannot go ahead and just design an amazing new application for the iPhone and send that out immediately to the vast iPhone community. Rather, everything that is designed for the iPhone must pass through the regulatory chains of the Apple corporation first. (Zittrain 2007) The rationale for this is that without this kind of extreme locking down,

virus- and bug-laden chaos would emerge, as has admittedly happened in the case of the PC (Zittrain, 2007). Jobs himself explains, "we define everything that is on the phone. You don't want your phone to be like a PC" (Zittrain, 2007, p. 2). It is in this sense, then, that the iPhone is not entirely generative: it lacks "a technology's overall capacity to produce unprompted change driven by large, varied, and uncoordinated audiences," (Zittrain, 2006, p. 7) as Jonathan Zittrain defines it.

This "appliancization" (Zittrain, 2006, p. 47) of technology may be likened to IBM's invention of the dedicated word processing appliance (Zittrain, 2006), which certainly provided greater security but was ultimately pushed off the market by PCs with word processing software. A similar fate may not necessarily await the iPhone, but certainly the iPhone represents an extreme solution to the openness problem in that generativity has, essentially, been lost.

Aside from the problem of closing it all down, there is also the other problem of keeping it all open. Undoubtedly, the combined force of open PC and Internet technology created – and continues to create – explosive generativity (Zittrain, 2006) that often provides great benefit to the public at large. The open PC has allowed independent programmers to create extremely helpful applications that are often better than any proprietary ones on the market while freely distributing them to other PC users. Concerning PCs, Zittrain (2006) states that "users who wrote their own software and thought it suited for general use could hang out

the shingle in the software business or simply share the software with others" (p. 11). The open Internet, similarly, has made its protocols publicly available. Programmers may therefore develop new Internet-based software or services and also distribute their creations freely, as "there is no central gatekeeper with which to negotiate access" (p. 15). The "uncompromising end-to-end neutrality" (p. 2) or "network neutrality" (p. 5) approach argues for the adherence to this network openness above and beyond all other considerations. "End-to-end" refers to the stance that Internet data transmission ought not to be interfered with by Internet Service Providers (ISPs) along any point in the exchange route and should merely be made to pass neutrally from one end of the network to the other as efficiently as possible (p. 16).

It therefore appears to make a lot of sense when Federal Communications Commission (FCC) chairman, Kevin J. Martin, says "we are preserving the open character of the Internet" (Hansell, 2008, ¶ 3) in response to questions concerning the FCC's 2008 vote to punish Comcast for perceived net neutrality violations. After all, why would anyone not want to retain these wonderful generative qualities of the Internet that are so clearly benefiting the public? As Zittrain (2006) suggests, "preserving the open character of the Internet" might actually require decisions that are entirely counter to upholding net neutrality (p. 5). The FCC at least seems to have the right motive here in that they are attempting to preserve generativity; however, many of those advocating a less heavy-handed approach to governance

than one that leads to appliancization would agree that there are better means of preserving generativity than enforcing unbound openness on the network.

Merely retaining the status quo – that is, keeping the Internet as open as it is – will ultimately result in more harm than good for the public. As Zittrain (2006) notes, an important point is that the Internet was initially developed by a *homogeneous base* of stakeholders. They all had the same interests in mind. Keeping the network entirely open was therefore seen as unproblematic, and "abuse of the network was of little worry because the people using it were the very people designing it – a culturally homogenous set of people bound by their desire to see the network work" (Zittrain, 2006, p. 16). Interestingly, that unfettered openness of the Internet seems to have remained despite the emergence of an entirely *heterogeneous base*. No longer is the Internet comprised of people with the same, or even remotely similar, motivations and competencies.

This leads us to the issue of the "bad code" conundrum (Zittrain, 2007, p. 5). The fact that any user may alter the inner workings of their PC at the mere click of a mouse is both a blessing and a burden. Certainly, without this availability, PC generativity would be hampered. But as Zittrain (2007) writes, "the PC user who clicks on bad code in effect hands over control of the PC to a total stranger" (p. 5). The prospect of infecting a network with viruses and worms therefore becomes heightened. In concert with the Internet, this vulnerability

becomes exacerbated. According to Zittrain (2006) "well-crafted worms and viruses routinely infect vast swaths of Internet-connected personal computers" (p. 6). It seems reasonable, then, to propose that a certain degree of data screening on behalf of the ISPs should be allowed (Zittrain, 2006). As long as ISPs are focusing on genuine problem areas such as this rather than getting sidetracked by technical minutiae such as domain names, positive results may be possible.

The Internet Corporation for Assigned Names and Numbers (ICANN) typifies the case of a corporation focusing too closely on technical minutiae (Klein, 2004, p. 9). "Too much scholarly effort has been devoted to the question of institutional governance of this small and shrinking aspect of the Internet landscape," writes Zittrain (2006) about domain name management (p. 6). For instance, if the people at ICANN channelled their energies less toward the market interests of domain names and more toward setting regulations for how ISPs should operate, they may have contributed more fruitfully to the online public domain (Klein, 2004). When an ISP detects that bad code is about to be transmitted through the network, then it should subvert that transmission. An ISP is, however, a company, and as Lawrence Lessig reminds us in a *Democracy Now!* interview, "companies are in the business of making money" (IWantDemocracyNow, 2008). He says, "if we begin to imagine a world where we trust companies to do good public policy, then we're fools because they'll do good public policy when

it makes sense for them from a financial perspective to do it" (IWantDemocracyNow, 2008). While this is not really arguable, avoiding any form of governance with a completely open network is still not the answer.

Companies will, however, respond to public uproar and make changes or opt not to make changes if their users express enough dissatisfaction. One example of this would be Facebook's 2009 attempt to change their terms of use policy for reasons of financial gain (Staff Writers, 2009). Owners of Facebook had hoped that their users would be accepting of a new policy that extended control over content even after account deletion. Thousands of users quickly petitioned against this proposed policy change and Facebook backed down. A similar system is needed to maintain Internet generativity, a public-private monitoring partnership, of sorts, in which members of the public continually mobilize private companies to take appropriate actions. Zittrain (2006) suggests:

> Tools can be developed to provide members of the general Internet public with simple but powerful information about the code they encounter. A hypothetical tool of this sort would be a dashboard displaying information such as how many other computers in the world were running a candidate piece of software and whether their users were on average more or less satisfied with their computers than those who did not run it. (p. 61)

To ignore the power of private companies and simply leave the management of these tools in the hands of the public, however, seems somewhat winsome. A public-private partnership would be the ideal construction, as then public policy concerns for the greater good may be efficiently actualized through the stability and expertise of private companies. The key word here is *continually*, because if the public again becomes complacent and lowers its expectations of ISPs, the old proponents of network neutrality will come racing back to the fore; suddenly cyberspace will be just as insecure as it once was.

Another major problem of complete end-to-end neutrality is "technologically guaranteed anonymity" (Zittrain, 2006, p. 65). The popular means of identifying individuals via tracking Internet Protocol (IP) addresses is clearly insufficient. One example is that of users surreptitiously obtaining free Internet connectivity from paying users on a wireless network. Zittrain (2006) writes, "...should outsiders use that connection, say, to send viruses or to pirate copyrighted files, the original consumer could be blamed when the Internet connection is traced" (p. 65). A greater degree of accountability is required to counteract this guaranteed anonymity. It should not be so difficult to identify who is responsible for inappropriate actions online. A proprietary, "closed source-style" (Simon, 2005, p. 231) shutting down of open contribution over the Internet would, however, hamper generativity and is therefore not an adequate solution. Instead, generativity could be maintained whilst imposing stronger governance on what happens over the network and who gets to upload what.

Zittrain's (2006) suggestion of the "license to code" (p. 52) could be a possible answer. Like a driver's license, this license to code would be open to acquisition by any Internet user with an interest in adding software to the network. One would not have to be an expert programmer to obtain a license; however, they would have to at least demonstrate a degree of competence. This competence may be demonstrated through the acquisition of positive feedback about one's work, much like in the case of eBay where new sellers slowly gain the trust of buyers. The policy would therefore not be so exclusionary as to hamper network generativity, as many non-expert users may still contribute innovations to the network. It would, though, weed out incompetent users who may be accidentally contributing bad code to the network and would also allow for easier identification of those acting negligently. A feedback-accepting database of programmers with this license to code could be linked with the aforementioned bad code reporting tool, allowing Internet users to verify that a file originated from someone with a license to code and that this programmer is in good standing with the bulk of the online community.

In many ways, this desire for accountability is what has contributed to the success of digital "gated communities" (Zittain, 2006, p. 58) such as Facebook and MySpace within the status quo of end-to-end neutrality on the Internet. Rather than attempting to deal with the uncertainty of the Internet as a whole, many people feel more comfortable with confining their regular Internet activity to a few

websites at most. Zittrain (2006) takes issue with these gated websites. He writes:

> ...From a generative standpoint, digital gated communities are prisons. Their confinement is less than obvious because what they block is generative possibility: the ability of outsiders to offer code and services to users, giving users and producers an opportunity to influence the future without a regulator's permission. (Zittrain, 2006, p. 58)

Merely perpetuating the development of these gated community websites, then, will lead to lost generative possibilities. An independent Facebook user, for instance, may develop a Facebook application that would benefit many users of the community, but it may never see the light of day if the Facebook bosses decide against its widespread implementation. Additionally, Facebook would ultimately have ownership privileges of the application, as it was built upon its framework. This constant and stifling requirement to go through and remain wedded to a higher power is, of course, non-existent on the wider generative Internet. There, perhaps with the added benefit of enhanced security provided by requiring a license to code, users may develop software and immediately distribute it globally without being tied down to a particular private entity such as Facebook.

What, then, is a viable alternative to the gated community on a secure, but generative Internet? The notion of a digital community with the functionality of Facebook, but regulated by the general public instead of a private company, gives rise to phenomenons such as Wikipedia. Zittrain (2009) writes in his blog that "Wikipedia licenses all its content so

that anyone can walk away with a copy of the whole encyclopedia and start a competing one at any time. Those who see Wikipedia governance as corrupt can take everyone's ball and start anew" (¶ 10). As Paul Duguid (2006) notes, however, Wikipedia has its problems. He writes, "inconsistencies [on Wikipedia] don't prevent contributions from either compiling or running. Hence small changes can easily run away with the coherence of the entry as a whole" (Duguid, 2006, ¶ 40). The aforementioned public-private partnership solution may be sufficient in getting private companies to adhere to newly-discussed public policy decisions, but it will likely not be sufficient in convincing them to transform their long-standing commitments to controlling user generativity. The lesser of two evils here may be the Wikipedia-like community idea, as generativity would not be as stifled as it would be under a traditional gated community. And perhaps, through the generativity of the community, users themselves may be encouraged to invent viable solutions to the well-documented problems of Wikipedia-like peer production (Duguid, 2006).

In what may be the most famous publication supporting the "uncompromising end-to-end neutrality" (Zittrain, 2006, p. 2) approach, John Perry Barlow (1996) writes that "we are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different" (¶ 5). Since this declaration was written over a decade ago, we may still reasonably ask the question: where is that promised governance? This idea of self-governance by Internet users does not seem to hold water in the wake of continuing online destabilization and ever-emerging threats to generativity. Perhaps one ought not to be so wary to liken the online situation to real world government; we could learn analogously from countries that have also struggled with dichotomous viewpoints, but managed to find a reasonable middle ground.

There are understandable motivations behind each extreme on this issue, but both parties are guilty of a kind of myopia. Those advocating for uncompromising openness on the network are rightfully concerned with maintaining generativity, but often they do not realize that blindly adhering to this openness may in fact have the opposite effect of stifling generativity (Zittrain, 2006). Those advocating for tethered appliancization and complete lock-down, on the other hand, are rightfully concerned with enhancing network security, but this would be at the cost of generativity. Both extremes might agree, then, that what is necessary is not a focus on openness, but whether or not the network is *securely generative*. A network that carefully, rather than heavy-handedly, imposes certain regulations on its users will be able to create and retain this kind of secure generativity. The creative pulse of the Internet will then become as incredibly healthy and innovative as it has the potential to be.

References

Barlow, J. P. (1996, February 9). A cyberspace independence declaration. Retrieved November 14, 2009, from Electronic Frontier Foundation: http://homes.eff.org/~barlow/Declaration-Final.html

Duguid, P. (2006). Limits of self-organization: peer production and laws of quality. First Monday, 11(10). Retrieved November 14, 2009, from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1405/1323

Hansell, S. (2008, August 2). F.C.C. vote sets precedent on unfettered web usage.

The New York Times. Retrieved November 14, 2009, from http://www.nytimes.com/2008/08/02/technology/02fcc.html

IWantDemocracyNow. (2008, April 18). Lawrence Lessig on Net Neutrality and Google-2/2 [Video file]. Video retrieved on November 14, 2009, posted to http://www.youtube.com/watch?v=DxQ0D0iW59o

Klein, H. (2004). ICANN and non-territorial sovereignty: Government without the nation state. Internet and Public Policy Project, 1-13.

Simon, K.D. (2005). The value of open standards and open-source software in government environments. IBM Systems Journal, 44(2), 227-38.

[Staff Writers]. (2009, February 19). Facebook backs down on controversial terms of use change. News.com.au. Retrieved November 14, 2009, from: http://www.news.com.au/write-facebooks-privacy-policy/story-0-1111118899666

Zittrain, J. (2006). The Generative Internet. Harvard Law Review, 119(I), 1-67.

Zittrain, J. (2007). Saving the Internet. Harvard Business Review, June, 1-10.

Zittrain, J. (2009, May 6). How to get what we all want. Retrieved 14 Nov. 2009, from Cato-unbound.org: http://www.cato-unbound.org/2009/05/06/jonathan-zittrain/how-to-get-what-we-all-want/