On the wrong side of order

The online world is no different from 'real' society in this regards. In the early 90s, the Internet was this proto-tribe or clan with no definite chieftains staking claim to territories. Netizens explored lands, settled down in areas where they found resources, formed communities, built tools and implements (web pages, software, applications), interacted with neighbors (in forums and groups) and mimicked certain characteristics of offline modes of communication, be it in individual expression, group behavior, networking, conducting business or indulging in leisure.

As I see it, there is inevitability to this trajectory and the Web would one day need gov- ernance. What accelerated external imposition of monitoring and regulations were other ac- cidental – and sometimes, deliberate – events that took place parallel to early net explora- tions. The first SPAM email was sent out on 3 May 1978; first “bootsector” virus Elk Cloner was released in 1981, affecting floppy disks; in 1984, William Gibson writes the book ‘Neu- roman’cer’ and coins the term ‘cyberspace’, effectively distancing the net from the edu- cational and scientific “classification” into the realm of pop-culture-science-fiction; by 1989 McAfee Associates were distributing free virus software.

It's in the mid-1990s, with the increasing rivalry between business corporations Microsoft, IBM, CISC0, Apple and Sun that we also see the first government and legal interventions in the arena of cyberspace and net technologies. Napster was created in 1999, incentivizing music sharing online and striking the matching of copyright and piracy wars. Also, in the same year, we experienced our first mass annihilation threat with the Y2K scare, and the year following, the ‘dotcom busts’ shook our bubble-grade faith in the invulnerability of the Web. In November 2001, The European Council adopts the first treaty addressing criminal of- fenses committed over the Internet.

So there you have it, our forays in cyberspace were never really about responsible discovery; criminality and juvenile behavior also went hand in hand. A simple example would be the annoying CAPTCHA’s that we have to pass through before our comments can be made visible on a blog. If spammers didn’t have so much leverage online or the tools to hood- wink the system, we wouldn’t need such check points, no? The same goes for piracy, phish- ing, money laundering, cyber-stalking, unso- licited pornography, hacking and disruption of secure, functional websites, and a host of other criminal activities that can’t be ignored or clicked away to the Recycle Bin.

The timeline to our current state is provided not as a history lesson and neither is it an ex- planation for the governments of the world to continue with their policies, which have steadil- y entered the territory of human rights abuse. With increasing criminal activities online – and increasing complaints from common man – the governments of the world have found it easy to take charge and gain footholds into our personal and private spaces. We now know more about surveillance, it’s not just a piece of brilliant fiction out of George Orwell’s mind. Everything from phone calls, messages to emails are censored, collated, archived, studied and sometimes, stopped from being sent out. Bloggers have been jailed, digital ac- tivists have been killed, net services have been shut down and services to websites have been denied arbitrarily. That moral high ground that I started off de- fending earlier has crumbled. Now, there is a tightening circle that we are pigeon-holed into and I no longer look to the ‘chief’ to keep me safe. The chief is in cohorts with the toolman (the group that harnesses technology to make weapons and design our security systems), lulling us into thinking that we cannot do with- out them. This stage is set for a showdown between techno-politico groups on one hand and civic-non-governmental factions on the other; one trying to hem us within boundaries, the other constantly redefining the meaning of boundaries. What gives you hope for a better cyber soci- ety? More difficult to answer, which side of the divide do you belong – the one that thrives in chaos or the one that seeks order? I am still toeing the line on this one.

As Pranesh Prakash puts it succinctly: “too little regulation and you ensure that criminal activities are carried on with impunity; too much regulation and you curb the utility of the medium.” But who do you turn to when the law makers make decisions even before you commit a crime? I guess there’s no ‘one- solution-fits-all’ answer. What you can bet your last buck on is that for every argument there’s a counter-argument. The anarchist who wants a law-less society is pitted against someone who wants balance and regulation through open data, open government and open culture initiatives. The cynic who is fed up of governmental control is pitted against the rationalist who calls for policy consultation with citizen-led groups. The poet who laments about surveillance might find solace with the academic stalwarts, who believe dialogue is a better way to achieve our aims - freedom with balance – than taking up arms.
No Tolls on The Internet

By Lawrence Lessig & Robert W. McChesney

Congress is about to cast a historic vote on the future of the Internet. It will decide whether the Internet remains a free and open technology fostering innovation, economic growth and democratic communication, or instead becomes the property of cable and phone companies that can put tollbooths at every on-ramp and exit on the information superhighway.

At the center of the debate is the most important public policy you’ve probably never heard of: “network neutrality.” Net neutrality means simply that all “like” Internet content must be treated “alike” (quote marks by me) and move at the same speed over the network. The owners of the Internet’s wires cannot discriminate. This is the simple but brilliant “end-to-end” design of the Internet that has made it such a powerful force for economic and social good. All of the intelligence and control is held by the users, not the networks that connect them. The protections that guaranteed network neutrality have been law since the birth of the Internet — right up until last year (2005), when the Federal Communications Commission (FCC) eliminated the rules that kept cable and phone companies from discriminating against content providers. This triggered a wave of announcements from phone company chiefs that they plan to do exactly that.

Now Congress faces a legislative decision.

Will we reinstate net neutrality and keep the Internet free? Or will we let die at the hands of network owners lurching to become content gatekeepers? The implications of permanently losing network neutrality could not be more serious. The current legislation, backed by companies such as AT&T, Verizon and Comcast, would allow the firms to create different tiers of online service. They would be able to sell access to the express lane to deep-pocketed corporations and relegate everyone else to the digital equivalent of a winding dirt road. Worse still, these gatekeepers would determine who gets premium treatment and who doesn’t.

Their idea is to stand between the content provider and the consumer, demanding a toll to guarantee quality delivery. It’s what Timotheus Huli, an Internet policy expert at Columbia University, calls “the Tony Soprano business model,” by extorting protection money from every website — from the smallest blogger to the largest corporation who gets premium treatment and who doesn’t.

Worse still, these gatekeepers would deter innovation. Without net neutrality, the Internet would start to look like cable TV. A handful of massive corporations would control access and distribution of content, deciding what you get to see and how much it costs.

As millions of citizens learn the facts, the message to Congress is clear: Save the Internet.

Lawrence Lessig is a law professor at Stanford University and founder of the Center for Internet and Society. Robert W. McChesney is a communications professor at the University of Illinois at Urbana-Champaign and co-founder of the media reform group Free Press.

Suffragette Surveillance, 1913

In 1912, Scotland Yard detectives bought their first camera, to covertly photograph suffragettes. The pictures were compiled into ID sheets for officers on the ground - BBC
Where the F**k Was I?

James Bridle

James Bridle has made another book from data, a printing-out-of-databases. This one is called “Where the F**k Was I?” and consists of 202 maps based on my movements over the past year.

I say “based on” because the data was not recorded by me, but by my phone. In April this year, researchers Alasdair Allen and Pete Warden revealed that the iPhone was storing location data without the user’s knowledge. Using their instructions and my own scripts, I extracted 35,801 latitude-longitude pairs stored on my phone between April and the previous June (when my phone was last updated, wiping its memory). These are plotted on OpenStreetMap, one map for each day, together with a brief note where I wanted to tie it to a real event.

I think this digital memory is better than mine—it frequently recalls things and places I’ve visited, without my knowledge. It is an approximation based on the device’s own “idea” of place. The app cross-references me with digital infrastructure, with cell towers and wireless networks, with points created by others in its database.

We share the city, and increasingly the world, with another network. The city is the abstraction machine, the digital networks, access points, substation data, and relay points, datacenters and fiber rings; its inhabitants are sensors and screens. Seeing through the machine’s eyes is a kind of breach: accessing a glossoply of the network.

This is an atlas, then, made by that other nature, seen through other eyes. But those eyes have been following me, unseen and without permission, and thus I consider provoking breach a necessary act. Perhaps how Kevin puts it, in a recent talk, reappropriated for the robots: “These are the astronomers for Earth, and they’re inventing new ways to see rather than things to look at. And rather than inventing new places to go, they’re inventing new ways to travel.”

Or this: At the Worlds Literature Festival (June 2011) in Norwich, the Sri Lankan-Canadian writer Shyam Selvadurai spoke of the space between his identities represented by that hyphen: a place where “the tectonic plates of cultures rub against one another, producing the eruption of my work.” Where Selvadurai is interested in the space between two human cultural identities, I suppose I am interested in the space where human and artificial cultures overlap (“artificial” is wrong, feels—what? Prejudiced? Colonial? Anthropocentric? Carbon-centric?).

There are no digital natives but the devices themselves, no digital immigrants but the devices too. They are a diaspora tentatively reaching out to the world, to understand it and themselves, and across the network to find and touch one another. This mapping is a byproduct, part of the process by which any of us, separate and indistinct long, find a place in the world.


NewsBytes

Perfect filtering of information on the Internet will lead to a fractured communication environment http://bit.ly/qZrINw

Andrew Keen: Compulsive sharing of everything through e-mail, Facebook, and Twitter are creating a personal diarrhea — Keen says “we are seeing the shadow of cyber regulation in the Internet.” http://bit.ly/2NhjKf

The (in)Visible Subject: Power, Privacy and Social Networking by Rebecca Schild

Schild argues that the interplay between privacy and power on social networks works individually to subject individuals to the gaze of surveillance, or to alternatively render them invisible. http://bit.ly/y4yEP

Privacy, By Design

For me, the most interesting questions to come out of Saturday’s open-space discussion of Privacy, By Design at CS were those around how to notice a privacy pact is constructed and negotiated. http://bit.ly/2OJDj

What next for privacy?

“The Internet is in a part a marketplace for horrific images of violent abuse. Should we say that, because these images are created and circulated via many different

Steps to exercising your rights

1. Go to your local ISP
2. Cut the message Go to your local ISP
3. Go crazy
4. Don’t get caught

Jail bloggers are alive and well. The Committee to Protect Journalists (CPJ) and the Arab Network for Human Rights Information today called on the Syrian government to produce immediate evidence showing that unjustly imprisoned blogger Tal-Al-Mallohi is alive and well. The demand follows several recent news reports saying that Al-Mallohi died in a Syrian prison a month ago.

http://www.ifex.org/2011/06/04/jailed_blogger/

Does the Internet inhibit democracy?

Video: http://www.youtube.com/watch?v=UdIiK5dVN7g

In this new RSA Animate adapted from a talk given in 2009, Evgeny Morozov presents an alternative take on “cyber-utopianism” — the seductive idea that the Internet plays a largely emancipatory role in global politics.

Let’s take back the Internet!

In this powerful talk from TEDGlobal, Rebeca MacKinnon describes the struggle for freedom and control in cyber-space, and asks: How do we design the next phase of the Internet with accountability and freedom at its core, rather than control?


Free Culture and Open Access initiatives don’t happen overnight and neither can they evolve purely in the realm of ideologies or revolutions. Let’s start by setting simple examples, says Samuel Tettner

One of the main issues that I think about under the broad umbrella of “Internet governance” is net neutrality. You all have heard me rant about the evils of private corporations and how they set an agenda that usually pain-inducing freedom & rights versus profits. At the workshop in Santiago [Feb 2011], I raised the issue of how private corporations do not recognize “citizens” but “consumers” as legitimate heirs of their ecosystems, at the heart of the Digital Age blogosphere. I also raised my fear about private corporations garnering too much power.

So, how do we move beyond concerns, fears and rants against big companies and powerful governments? How do we champion the openness initiative? In my case, I was a good starting point for myself as I decided to put the idea of openness into action. For this issue of “Links in the Chain”, I created an information sheet similar to the one you would see on an NGO handbook: a manifesto of sorts (see image above), highlighting my goals, the method and the process of this exercise. The actual implementation involved getting the team to work together, share ideas and information, especially de-centralization — where one person doesn’t control the entire workflow.

Of course, in the complex world we live in, the specifics of an open cultural or political system is not as simple as printing out a sign and needing to be fleshed out in detail. For example, is it worth asking if there are types of information that should not be open to everyone for security reasons? Having open access to government budget allocations and private campaign contributions would increase accountability, but is it equally useful to know about future military developments?

It is also important to understand the extent of the overall information network that specifies the conditions of impact players have. If an ISP that provides access to 15% of the internet population decides to impose limitations on websites that people can visit, can the misinformation effects be traced and mapped on a larger scale? It is the case that for Internet governance today, public and private interest and jurisdictions have bled into each other and created a situation in which the role of private ISPs is crucial to the proper functioning of an information democracy.

The idea for me is to: start talking about — and implementing — the culture of free and open access to the Internet and promote a transparent information ecosystem more as a fundamental right and feature of modern democracies rather than a commoditized service. This will curtail some of the restrictions and barriers that ISPs are allowed to institute. It sounds grandiose but such a perceptual shift would be very helpful.

Call for participation


NEWSBYTES

The shadow of cyber regulation

In response to growing Internet security concerns, governments are working toward further regulation, with the end result possibly being its fragmentation into discrete national networks. To avoid such fragmentation, the Internet states should negotiate a framework convention on cyberspace.


Australia, Seeks To Censor The Internet

After much pressure from the Australian government, the country’s two largest ISPs, Telstra and Optus, along with two smaller ISPs (iBlast and WestTel) have agreed to start censoring the internet, blocking a secret list of websites from view. This is the “artificial” is wrong, feels—what? Prejudiced? Colonial? Anthropocentric? Carbon-centric?...
Whistleblower

The recent disclosures from Wikileaks have shown that the right to information, whistle-blowing, and privacy are interconnected.

Enonal Micki looks at the different ways in which the three are related, as well as looking at the benefits and drawbacks to Wikileaks in terms of privacy.

Introduction

A recent interview, the Canadian Privacy Commissioner was quoted as saying “Information and the manipulation of information is one of the most powerful tools. Those who are in control of the information can influence society enormously.”

History and present-day society have both seen the truth in this statement. Of course, among many reasons that the right to information is important to uphold is in India, and in other countries, there are statutes – in India, the Right to Information Act – that entitle the public to request and receive information that pertains to public bodies and their conduct, in formation that is publicly available.

An entirely separate but equally critical way in which Wikileaks is at play is through whistle-blowing. Traditionally, whistle-blowing is any disclosure made in the name of public interest, recent events such as the leaks of US diplomatic cables have brought to light the relationship between the public’s right to information, the rights of whistleblowers, and the rights of individuals to privacy. These recent cases have shown that the right to privacy, whistle-blowing, and the right to privacy are all interconnected, because privacy can provide individuals with the means to sustain autonomy against potentially overwhelming forces of government and persons who might have mixed motivations.

One of the key questions that Wikileaks raises is this: if whistle-blowing is supposed to be disclosed through the public interest, i.e., to protect the public – should disclosure of personal information be permissible only if a person can demonstrate that he/she is trying to protect the public or avoid actual wrongdoing rather than simply protect information that is “interesting to the public?”

What is a whistleblower and how does a whistleblower benefit from Wikileaks?

Whistleblowing is the modern counterpart to “informers” – people who reveal others’ wrongdoing. For example, countries, a person may have in his/her possession important information of a whistle-blowing nature to a judicial body. The judicial body then determines the veracity of the information, the degree of public interest involved, and the proper form of action to be taken. The judicial body also offers legal protection to the whistleblower. Another method of whistleblowing is to leak information to the public directly. Once information is in the public domain – at least if there is freedom of press – there are no controls over it. Neither the right to free press, nor the right to protection as a whistleblower is universal.

The current critique of the Indian Whistle-blowing Bill is that the right to protection will not be ensured & A Times of India (newspaper) article issued in September 2010 points out that the Whistle-Blowing Act’s biggest weakness is that the Bill’s Central Vigilance Commission is designated to play both the role of compe- tent authority to deal with complaints filed by whistleblowers and as the tribunal to protect whistleblowers. Structuring the power to allow a conflict of interest would not be conducive to the legal needs and bias could breed distrust that would cause people to avoid the system altogether.

In these situations, Wikileaks is an interesting and powerful tool for individuals who either want to remain anonymous, or do not want to be burned by a public trial. However, Wikileaks’ ability to leak information can influence society enormously.

With the 2011 Internet Governance Forum (IGF) slated for a September run this year, Nigeria, Singapore, Sri Lanka, Tanzania, and Malaysia are all preparing for their first appearances. Indonesia, Pakistan, and Singapore last year where she argued for a proactive UN engagement with women & youth. In Nepal, the government has been criticized for withholding the data but the fact that this is not precisely the same because it is not a one stop shop, but instead is a way for a person to post information on a mass media outlet. It should be noted, however, that informants who leak to Wikileaks are not afforded the same immunities and the same legal protections that whistleblowers are granted. When an individual shares documents or information with Wikileaks, the site in turn publishes the information on the web and with the press.

Privacy and Whistleblowing

When looking at the act of whistleblowing through the lens of privacy, there are obvious privacy concerns for the whistleblower, for the person or entity whose information has been leaked, and for possible third parties also. One of the major challenges for the Privacy Commissioner, pointed out that for the whistleblower, the integrity and identity, safety and reputation of the alleged wrongdoer, and third parties, can be undermined. The alleged wrongdoer, the individual’s identity and safety. For the alleged wrongdoer, the privacy concerns include identity, safety, employment, and liberty (where sanctions may include imprisonment). For third parties, reputation and safety can both be compromised. Where the whistleblower publishes information that is not public knowledge, the individual is subjected to attack in the public domain.

Even though Wikileaks works to protect the anonymity of individuals who leak information, it is not binding by any law to protect the privacy of individuals involved in the leak. The concept behind Wikileaks is that by releasing information, there is the ability to bring accountability and transparency to governing bodies, but the only regulation over Wikileaks is internal (and thus inherently subjective) – Wikileaks needs to change its structure to take into account leaks shared without the intent of protecting the public interest and even then needs to monitor to prevent leaks that might affect national security, safety, or disclo- sions or damage reputations with no validating information.

The Internet Governance Forum (IGF) is scheduled to take place in November this year, Nigeria, Singapore, Tanzania, and Malaysia are all preparing for their first appearances. Indonesia, Pakistan, and Singapore last year where she argued for a proactive UN engagement with women & youth. In Nepal, the government has been criticized for withholding the data but the fact that this is not precisely the same because it is not a one stop shop, but instead is a way for a person to post information on a mass media outlet. It should be noted, however, that informants who leak to Wikileaks are not afforded the same immunities and the same legal protections that whistleblowers are granted. When an individual shares documents or information with Wikileaks, the site in turn publishes the information on the web and with the press.

Privacy and Whistleblowing

When looking at the act of whistleblowing through the lens of privacy, there are obvious privacy concerns for the whistleblower, for the person or entity whose information has been leaked, and for possible third parties also. One of the major challenges for the Privacy Commissioner, pointed out that for the whistleblower, the integrity and identity, safety and reputation of the alleged wrongdoer, and third parties, can be undermined. The alleged wrongdoer, the individual’s identity and safety. For the alleged wrongdoer, the privacy concerns include identity, safety, employment, and liberty (where sanctions may include imprisonment). For third parties, reputation and safety can both be compromised. Where the whistleblower publishes information that is not public knowledge, the individual is subjected to attack in the public domain.

Even though Wikileaks works to protect the anonymity of individuals who leak information, it is not binding by any law to protect the privacy of individuals involved in the leak. The concept behind Wikileaks is that by releasing information, there is the ability to bring accountability and transparency to governing bodies, but the only regulation over Wikileaks is internal (and thus inherently subjective) – Wikileaks needs to change its structure to take into account leaks shared without the intent of protecting the public interest and even then needs to monitor to prevent leaks that might affect national security, safety, or disclosures or damage reputations with no validating information.

With the 2011 Internet Governance Forum (IGF) slated for a September run this year, Nigeria, Singapore, Tanzania, and Malaysia are all preparing for their first appearances. Indonesia, Pakistan, and Singapore last year where she argued for a proactive UN engagement with women & youth. In Nepal, the government has been criticized for withholding the data but the fact that this is not precisely the same because it is not a one stop shop, but instead is a way for a person to post information on a mass media outlet. It should be noted, however, that informants who leak to Wikileaks are not afforded the same immunities and the same legal protections that whistleblowers are granted. When an individual shares documents or information with Wikileaks, the site in turn publishes the information on the web and with the press.

Privacy and Whistleblowing

When looking at the act of whistleblowing through the lens of privacy, there are obvious privacy concerns for the whistleblower, for the person or entity whose information has been leaked, and for possible third parties also. One of the major challenges for the Privacy Commissioner, pointed out that for the whistleblower, the integrity and identity, safety and reputation of the alleged wrongdoer, and third parties, can be undermined. The alleged wrongdoer, the individual’s identity and safety. For the alleged wrongdoer, the privacy concerns include identity, safety, employment, and liberty (where sanctions may include imprisonment). For third parties, reputation and safety can both be compromised. Where the whistleblower publishes information that is not public knowledge, the individual is subjected to attack in the public domain.

Even though Wikileaks works to protect the anonymity of individuals who leak information, it is not binding by any law to protect the privacy of individuals involved in the leak. The concept behind Wikileaks is that by releasing information, there is the ability to bring accountability and transparency to governing bodies, but the only regulation over Wikileaks is internal (and thus inherently subjective) – Wikileaks needs to change its structure to take into account leaks shared without the intent of protecting the public interest and even then needs to monitor to prevent leaks that might affect national security, safety, or disclosures or damage reputations with no validating information.

With the 2011 Internet Governance Forum (IGF) slated for a September run this year, Nigeria, Singapore, Tanzania, and Malaysia are all preparing for their first appearances. Indonesia, Pakistan, and Singapore last year where she argued for a proactive UN engagement with women & youth. In Nepal, the government has been criticized for withholding the data but the fact that this is not precisely the same because it is not a one stop shop, but instead is a way for a person to post information on a mass media outlet. It should be noted, however, that informants who leak to Wikileaks are not afforded the same immunities and the same legal protections that whistleblowers are granted. When an individual shares documents or information with Wikileaks, the site in turn publishes the information on the web and with the press.

Privacy and Whistleblowing

When looking at the act of whistleblowing through the lens of privacy, there are obvious privacy concerns for the whistleblower, for the person or entity whose information has been leaked, and for possible third parties also. One of the major challenges for the Privacy Commissioner, pointed out that for the whistleblower, the integrity and identity, safety and reputation of the alleged wrongdoer, and third parties, can be undermined. The alleged wrongdoer, the individual’s identity and safety. For the alleged wrongdoer, the privacy concerns include identity, safety, employment, and liberty (where sanctions may include imprisonment). For third parties, reputation and safety can both be compromised. Where the whistleblower publishes information that is not public knowledge, the individual is subjected to attack in the public domain.

Even though Wikileaks works to protect the anonymity of individuals who leak information, it is not binding by any law to protect the privacy of individuals involved in the leak. The concept behind Wikileaks is that by releasing information, there is the ability to bring accountability and transparency to governing bodies, but the only regulation over Wikileaks is internal (and thus inherently subjective) – Wikileaks needs to change its structure to take into account leaks shared without the intent of protecting the public interest and even then needs to monitor to prevent leaks that might affect national security, safety, or disclosures or damage reputations with no validating information.
Being a Reluctant Anarchist

Could anarchy be the answer to the political turmoil and disenchantment of modern society? Alaa Abd El-Fatah reflects about ‘dispossession’ as a means of being in control.

Recently, I discovered that there are aspects of myself that I was very attached to. It is true that I have been abroad back home in Egypt, but they reflect an attachment to a particular culture that was always spreading while I was away. Today I live in South Africa, and I find myself feeling constantly dispossessed of them.

I have been mitigating this ‘loss’ by over expressing some of it online and it’s turning into a loud, incessant and boring voice. Being alienated from my blog is making things worse, as I longly express myself in the very limited and crippling medium of Twitter (I really don’t get people who champion the 140-character limit to communicate).

So I came to the Digital Natives workshop with my own personal agenda. I wanted to use it as a space to learn to express these aspects in English, and outside of my own context. With this agenda in mind, I chose the word “Dispossession” to express my political identity in a word-matching activity. “The Dispossessed” is the title of a science fiction novel by Ursula K. Le Guin, about a truly anarchistic human society, living without government, power hierarchies or private property.

Dispossession

In Ursula’s novel, dispossession is a positive and negative aspect. As an activist is full of optimism, but entirely un-governance. They are (and I enjoy these activities). I find myself very able to imagine the world Ursula saw dispossession as positive.

Dispossession, hierarchies or private property. While I am unable to imagine a move from South Africa, I find myself feeling constantly ally expressed while traveling. Now that I live in South Africa, I find myself feeling constantly dispossessed of them.

entrants and a choice. But I also chose the word “Imagination.” I’m a reluctant anarchist: I don’t buy any of the arguments that justify states, borders, capital or governments; I abhor power in all its forms”

Passion and Hope

Evelyn from Zimbabwe chose restoration to symbolize the need for Zimbabweans to re-store their sense of power, their control over their destinies and livelihoods. We first dis-covered how power is always within the people. All power is derived from the masses but we seem to need to reclaim that constantly. I tried to imagine the situation in Zimbabwe (despite all its horrors) in a positive way – the way Ursula saw dispossession as positive.

And activism is at its essence a practice in mytholog: We have to invent an unreal world, and imagine it being possible. Then, we invent ways to get there and it is the strength of that belief that carries us closer to our goals.

I guess this has been my frustration with South Africa. I read the freedom charter and I brought tears to my eyes that such a doc-ument can be imagined collectively by a people living under such harsh political conditions. I read blogs and newspapers today and feel nothing but anger that a people living in liberty can’t be bothered with imagination.

Bullshit

My friend Amine from Morocco touched a nerve here, talking about the layers of deceit and bullshit we all engage in even as activists. Do we truly know who we are? What we want? What is our agenda? Are we working for the change we say we are working for? Are we liv-ing the change we want to be? What are our true agendas?

This resonated with the reluctant part of my anarchism. Is the gulf between my reality and my dream just bullshit? Even on a more personal level, am I a true feminist like I want to think of myself or is my relationship with my wife a replication of the power dynamics I ab-hor?

To Amine, the important thing is that you engage in the process of self reflection and examination that explores your bullshit. We talked about how this matters on the personal level more than the collective. The motivations of each individual in a movement are not es-sentially relevant to the success or failure of that movement; good positive change can happen despite all our petty failings.

To read the full version of this write-up, visit: http://bit.ly/AmPhpSpk.

Written in the Hindi language by Indian poet Pradeep Madhok, the poem bids a fond farewell to McSpeedy, the courier pigeon.

Colombia’s Copyright Bill 241

Mauricio Fino Garzon gives us the lowdown on a new copyright bill filed by his country’s Congress.

The Contrarian View

Accolade for McSpeedy

The local version: using social networking and the dynamics that create groups and larger platforms that generated the internet. It is a new age of social and political movements.

The real question: are these platforms (like Facebook) to be the new public square? Are they the new public awareness instruments? Who are the new public artists and new public audiences of artists?

For McSpeedy I write in praise, Let me end my email here
The Draft folder is now clear.

applying a penal system that has been traditionally applied only to a few, but which is quite extensive in this country.

The Contrarian View

Could anarchy be the answer to the political turmoil and disenchantment of modern society? Alaa Abd El-Fatah reflects about ‘dispossession’ as a means of being in control.

Recently, I discovered that there are aspects of myself that I was very attached to. It is true that I have been abroad back home in Egypt, but they reflect an attachment to a particular culture that was always spreading while I was away. Today I live in South Africa, and I find myself feeling constantly dispossessed of them.

I have been mitigating this ‘loss’ by over expressing some of it online and it’s turning into a loud, incessant and boring voice. Being alienated from my blog is making things worse, as I longly express myself in the very limited and crippling medium of Twitter (I really don’t get people who champion the 140-character limit to communicate).

So I came to the Digital Natives workshop with my own personal agenda. I wanted to use it as a space to learn to express these aspects in English, and outside of my own context. With this agenda in mind, I chose the word “Dispossession” to express my political identity in a word-matching activity. “The Dispossessed” is the title of a science fiction novel by Ursula K. Le Guin, about a truly anarchistic human society, living without government, power hierarchies or private property.

Dispossession

In Ursula’s novel, dispossession is a positive and negative aspect. As an activist is full of optimis-
When the law respects the right to freedom of expression and the right to information, it is crucial for the development of a democratic and prosperous society. The Indian government has a responsibility to protect the interests of all citizens, including internet users, and to ensure that their rights are respected. This requires a careful balance between the need for security and the need for freedom. The proposed internet regulation bill in India is a step in the right direction, as it seeks to protect the interests of all citizens and to ensure that the internet is used for the benefit of all. However, it is important that the bill is carefully scrutinized and that its provisions are carefully monitored to ensure that they are in line with international standards and with the principles of democracy and human rights.

In conclusion, the internet is a vital tool for communication, education, and entertainment, and it should be protected and regulated in a way that respects the rights of all citizens. The Indian government has a responsibility to ensure that the internet is used for the benefit of all, and it should work closely with citizens and civil society organizations to develop a framework that respects the rights of all citizens and that is in line with international standards.
You have the right to remain silent

India has a long history of censorship that it justifies in the name of national security, but new laws governing the Internet are unnecessary and—given the multitude of online voices—is thought through, says Anja Kovacs

I n March 2011, Indian media – both social and traditional — was abashed with fear that a new set of rules, proposed to complement the IT (Amendment) Act 2008, would thwart the freedom of expression of India’s bloggers. Contrary to standard international practice, the Intermediary Liability Divulgence Rules seemed intent on making bloggers responsible for comments made by readers on their site. Only a few weeks earlier the threat of online censorship had manifested itself in a different form: although the blog was implemented unevenly, mobile applications market space. Mobango, bulk SMS provider, and blogs hosted on Typepad were suddenly no longer accessible for most Indian netizens, without warning or explanation.

An appetite for censorship does not only exist among India’s legislature and judiciary; however. Especially since the early nineties when instances of vigilante groups destroying art, preventing film screenings, or even attacks on individuals without warning or explanation, especially since the nineties, blogs, and social networking sites have seen increased regulatory activity. The authority to allow or block access to any entity at any time and for any reason had thus far been exercised with relative impunity. Social networking sites in particular, as they host so much content, have been targeted increasingly. But it is not the only type of content that is subject to outright prohibition. What kinds of terms of service? It will require intermediaries to bar users from posting messages that they regard as “false,” it doesn’t cover only intermediaries that are public-facing. So this means that your forwarding a joke via e-mail, which “belongs to someone and to which the user does not have any right” will be deemed to be in violation of the law (such as betting on horses) isn’t banned in India and casino gambling is legal in Goa, for example; under these Rules, all speech ‘promoting gambling’ is prohibited.

The rules are very onerous on intermediaries, since they require them to act within 36 hours to disable access to any information that they receive a complaint about. Like many affected online intermediaries will now play the role that judges have traditionally played. Any affected person can bring forth a complaint about issues as diverse as defamation, blasphemy, trademark infringement, threatening or inciting integrity of India, ‘disparaging speech’, or the blanket ‘in violation of any law’. It is not made mandatory to give the actual violator an opportunity to be heard, thus violating the formal principle of natural justice of ‘hearing the other party’ before denying them a fundamental right. Many of the rules’ architects are turned off by the legal norms implicit in the public service obligation. This is an issue that the law’s ambit. In this context, even if it may still have a role, suppression clearly can no longer be the preferred or even dominant technology of choice to manage disagreements. What is urgently needed is the building of a much stronger culture of respectful disagreement and debate within and across the country’s many social groups. If more and more people are now getting an opportunity to speak, what we need to make sure is that they end up having a conversation.

Yet the government of India so far has not shown any signs of changing track, putting into place a range of legislations and polices to meticulously monitor and police within its borders. Thus, for example, section 66A(b) of the IT (Amendment) Act 2008 defines ‘cyberterrorism’ so broadly as to include the unauthorised access to information on a computer with a view to...denigrating India’s image.

The proposed Cyber Cafe Rules 2011 order that children who do not possess a photo identity card need to be accompanied by an adult who does, constrain the Internet access of young people among the less advanced sections of society in particular. And while the US and other Western countries continue to debate the desirability of an Internet kill switch, the Indian government obtained this prerogative through section 69A of the IT (Amendment) Act 2008 years ago.

Proponents of such legislation often point to the new threats to safety and security that the Internet poses to defend these measures, and it is indeed a core obligation of any state to ensure the safety of its citizens. But the hallmark of a democracy is that it carefully balances any measures to do so with the continued guarantee of its citizens’ fundamental rights. Despite the enormous changes and challenges that the complainer without preference to apply their energy where, such an exercise seems to sadly not yet have been systematically undertaken in India so far.

Excerpts from an article written for The Sunday Guardian.

You have the right to remain silent. Wrong. It is a legal right. But it is a legal right only in the sense one is not required to reveal one’s name and address, or communication link made available or hosted. It qualifies by stating that they are not liable if they follow certain precautions (basically, to show that they are real intermediaries). They observe blue dilution and don’t exercise an editorial role; they don’t help or induce commission of the unlawful act; and aren’t receiving legal knowledge, or on being duly notified by the appropriate authority, the intermediary steps towards some kind of action.

So, rules were needed to clarify what blue dilution involves (i.e., to state that no active monitoring is required of ISPs), what actual knowledge means, and to clarify what happens in happens in case of conflicts between this provision and other parts of IT and other Acts.

Impact on freedom of speech and privacy

However, that is not what the rules do. The rules instead propose standard terms of service to be notified by all intermediaries. This means everyone from Airtel to Hotmail to Facebook to Rediff blogs to You Tube, to organizations and people who allow online comments, to post comments on their website. What kinds of

R egiulation of the Internet, as with regulation of any medium or speech and commerce, is balancing act. Too little regulation and you curtail the industry to a point of no viability; too much regulation and you curtail the utility of the medium. This is especially so with the Internet, as it has managed to be the impressively vibrant space it is due to a choiceful care in most countries of eschewing over-regulation. India, however, seems to be taking a different turn with a three sets of new rules under the Information Technology Act.

These rules deal with the liability of intermediaries (i.e., a large, inclusive, groups of entities and individuals that transmit and allow access to third-party content). Intermediaries, who safeguard content, if they are not to be held liable for their users’ activities, and the practices that intermediaries need to follow to ensure security and privacy of customer data.

What does the Act require?

Section 79 of the IT Act states that intermediaries are generally not liable for third party information, data.

Also propose standard terms of service to be notified by all intermediaries. This means everyone from Airtel to Hotmail to Facebook to Rediff blogs to You Tube, to organizations and people who allow online comments, to post comments on their website. What kinds of

You have the right to remain silent

India has a long history of censorship that it justifies in the name of national security, but new laws governing the Internet are unnecessary and — given the multitude of online voices — is thought through, says Anja Kovacs

I n March 2011, Indian media – both social and traditional — was abashed with fear that a new set of rules, proposed to complement the IT (Amendment) Act 2008, would thwart the freedom of expression of India’s bloggers. Contrary to standard international practice, the Intermediary Liability Divulgence Rules seemed intent on making bloggers responsible for comments made by readers on their site. Only a few weeks earlier the threat of online censorship had manifested itself in a different form: although the blog was implemented unevenly, mobile applications market space. Mobango, bulk SMS provider, Clickatell, hacking-related portal Zone-H.com and blogs hosted on Typepad were suddenly no longer accessible for most Indian netizens, without warning or explanation.

An appetite for censorship does not only exist among India’s legislature and judiciary; however. Especially since the early nineties when instances of vigilante groups destroying art, preventing film screenings, or even attacks on individuals without warning or explanation.

What does the Act require?

Section 79 of the IT Act states that intermediaries are generally not liable for third party information, data.

Also propose standard terms of service to be notified by all intermediaries. This means everyone from Airtel to Hotmail to Facebook to Rediff blogs to You Tube, to organizations and people who allow online comments, to post comments on their website. What kinds of

You have the right to remain silent

India has a long history of censorship that it justifies in the name of national security, but new laws governing the Internet are unnecessary and — given the multitude of online voices — is thought through, says Anja Kovacs

I n March 2011, Indian media – both social and traditional — was abashed with fear that a new set of rules, proposed to complement the IT (Amendment) Act 2008, would thwart the freedom of expression of India’s bloggers. Contrary to standard international practice, the Intermediary Liability Divulgence Rules seemed intent on making bloggers responsible for comments made by readers on their site. Only a few weeks earlier the threat of online censorship had manifested itself in a different form: although the blog was implemented unevenly, mobile applications market space. Mobango, bulk SMS provider, Clickatell, hacking-related portal Zone-H.com and blogs hosted on Typepad were suddenly no longer accessible for most Indian netizens, without warning or explanation.

An appetite for censorship does not only exist among India’s legislature and judiciary; however. Especially since the early nineties when instances of vigilante groups destroying art, preventing film screenings, or even attacks on individuals without warning or explanation.
The parts of a poem were so constructed by four co-authors who lived thousands of miles apart, in diverse global locations with their hearts-in-minds-unitedly-working, to the texture of a simple affirmation... of LIFE.

So, on an FB status message they piloted, line after line, in quietly rejoicing proximity. Below the Panda's status message, the Piggy posted a comment, the little glowing anger, and a Spelling Bee followed. Posting LineAfterLine, making lyrical progression. The poetry jam and butter was sandwiched to a final version. It was a sight to behold! Their ping-like-click fest turning LIVE into a blessed poem!

But | but | but | but | but | err, the piggy butted in "POST PRODUCTION.

Piggy said, "Give it to me now!"

Piggy nearly caused a little pow-pow POST PRODUCTION.

The parts of a poem were so constructed by four co-authors who lived thousands of miles apart, in diverse localities with their hearts-in-minds-unitedly-working, to the texture of a simple affirmation... of LIFE.

So, on an FB status message they piloted, line after line, in quietly rejoicing proximity. Below the Panda’s status message, the Piggy posted a comment, the little glowing anger, and a Spelling Bee followed. Posting LineAfterLine, making lyrical progression. The poetry jam and butter was sandwiched to a final version. It was a sight to behold! Their ping-like-click fest turning LIVE into a blessed poem!

But | but | but | but | but | err, the piggy butted in "POST PRODUCTION.

Piggy said, "Give it to me now!"

Piggy nearly caused a little pow-pow POST PRODUCTION.