digital natives

Links in the Chain

A Newsletter of the Digital Natives with a Cause? Project

Vol. 8 Issue II

MID-YEAR EDITION SPECIAL LINKS IN THE CHAIN

Editorial Net Governance & Regulation

On the wrong side of order

GUEST EDITOR: Nilofar Ansher | India
Journalist | Editor | Digital Native |
Blog: http://www.trailofpapercuts.wordpress.com |
Twitter: @culture_curate

Try as I might, I am unable to climb out of a clichéd well of parables and phrases when it comes to piecing together a coherent write-up on 'net governance and online regulation'. My thoughts are insistent on driving home the point about 'great power and great responsibility', 'you sow what you reap', 'freedom is never won, you earn it', 'your freedom ends where my nose begins' – you get the drift – a pronouncedly moral poker stokes this fireplace.

So, how do I come off on a moral high ground and err on the side of governance, especially since I label myself a digital native – a post-modern netizen, and therefore (perhaps, irrationally), subscriber to all things free, open and even anarchic? And yes, this is a battle and there are sides. Either you want a cyberspace with curfews and lock downs or a Wild West Frontier, where it's a free for all.

Perhaps a call for governance comes from a self-defined righteousness of the situation. I consider myself in danger (will come to this later), and so, think it's my moral right to ask for protection. In turn, it's the duty of the government to protect me. Built-in are the dialectics of trust and responsibility, freedom and power, order and privacy, safety and intrusion; these antonyms constantly warring with each other in a space that is nebulous - and virtual. Unlike statehood or borders to a city, the boundaries of virtual cities are not staked to rulers yet.

History has taught us that no town or village, no city or state progresses without the creation and evolution of complex political structures of control and regulation. A burgeoning population signals the arrival of crime in various degrees and we turn to a single entity to set things in order. It's a different matter that those in power also wreck havoc, however, it's also true that a diverse set of people competing for the same resources do not adhere to reason - they subscribe to governance.

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 behaviour, networking, conducting business or indulging in leisure.

As I see it, there is inevitability to this trajectory and the Web would one day need governance. What accelerated external imposition of monitoring and regulations were other accidental – and sometimes, deliberate – events that took place parallel to early net explorations. 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 'Neuromancer' and coins the term 'cyberspace', effectively distancing the net from the educational 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, CISCO, 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 thrill 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 offenses 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 CAPTCHAs 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 hoodwink the system, we wouldn't need such check points, no? The same goes for piracy, phishing, money laundering, cyber-stalking, unsolicited 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 explanation for the governments of the world to continue with their policies, which have steadily 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 activists 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 defending 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 without them. The 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 society? 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 judge you guilty 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.

CONTRIBUTORS

Pradeep Madhok | India
Morning: Assistant Manager @ Schneider Electric | Evening: poet @ http://wo-khwab.blogspot.com

Dr. Anja Kovacs |Delhi, India
| Movements. Activism. Technology. Research. Feminism. Marxism. Change. Fellow at the Centre for Internet and Society, Bangalore
| Email: anja@cis-india.org | Twitter: @anjakovacs

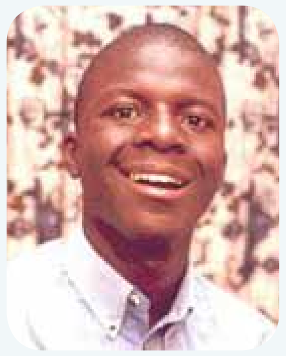
Samuel Tettner | USA / Europe
Researcher @CIS-India | Venezuelan Jew who studied in the US | Science & Technology, knowledge, networks, innovation, and governance | Blog: http://tettner.com |
Twitter: @Tettner

James Bridle | UK
Author of 'Where the F**k Was I? (A Book)" | Has worked in a number of roles within and outside the publishing industry, from publicity and marketing to editorial, and from online strategy to web application development and production | Website: http://booktwo.org |
Twitter: @jamesbridle

Simeon Oriko | Nairobi, Kenya
The boy who changed the world | founder and executive director of @TheKuyuProject & @StorySpacesHQ | Website: http://mtotowajirani.com | Twitter: @mtotowajirani

ALBERT MUCUNGUZI
(Uganda) Founder, PC Tech Magazine Blogger | Director of Strategy and Business Development at PC Tech Communications Ltd.
Web/Blog: http://almuc.me/blog |
Twitter: @albertmuc

Elonnoi Hickock | India
Policy and Advocacy Advocate @cis_india |
Researcher at Privacy India
Website: http://privacyindia.org/ |
Email: elonnai@cis-indis.org



James Mlambo | Harare, Zimbabwe
Tech support, budding programmer | ICT action hero for kids and youth @CyberGateway
Websites: http://jamesmlambo.htmlplanet.com/index.html & www.cybercentre.freeservers.com |
Twitter: @james_mlambo

Mauricio Fino Garzón | Bogota, Colombia
Profesional en ciencia de la información - bibliotecólogo, interesado en el infoactivismo y con ganas de ser backpacker // Professional information science librarian, interested in InfoActivism & willing to be backpacker |
Twitter @maolibrarian

Pranesh Prakash | Bangalore, India
Policy wonk | Works on issues of IP reform, 'openness', freedom of expression, and transparency at the Centre for Internet and Society | Twitter: @pranesh_prakash / @cis_india

Alaa Abd El-Fatah
Egypt | Pretoria, South Africa | Egyptian blogger, software developer, and political activist Web: http://www.manalaa.net/ |
Twitter: @alaa

Hasina Hasan | India | Poet | critic | Magic Mistress | Midnight Hauntress | Activist | Performer | Epicurious
Blog: http://sinasan.wordpress.com |
Twitter: @wontonwarrior

María del Mar Zavala | Asunción, Paraguay
Member of the Environmental Law and Economics Institute (Instituto de Derecho y Economía Ambiental-Paraguay) |
Twitter: @tuyuyuPY

Nighat Dad | Pakistan
TakeBackTheTech Campaigner | Privacy Activist | Public Policy Researcher | Special Public Prosecutor | Human Rights Activist |
Twitter: @nighatdad

Prashant Iyengar | India
Head researcher at Privacy India and researcher @cis_india |
Email: prashantiyengar@gmail.com

Blast From the Past

No Tolls on The Internet

Excerpts from the article written for The Washington Post on Thursday, June 8, 2006

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 toll booths 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 producers and 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 chief executives 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 it die at the hands of network owners itching 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 Timothy Wu, 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 Google – network owners would earn huge profits. Meanwhile, they could slow or even block sites and services of their competitors or those who refuse to pay up. They'd like Congress to "trust them" to behave.

Without net neutrality, the Internet would start to look like cable TV. A handful of massive companies would control access and distribution of content, deciding what you get to see and how much it costs. Major industries such as health care, finance, retailing and gambling would face huge tariffs for fast, secure Internet use – all subject to discriminatory and exclusive deal-making with telephone and cable giants.

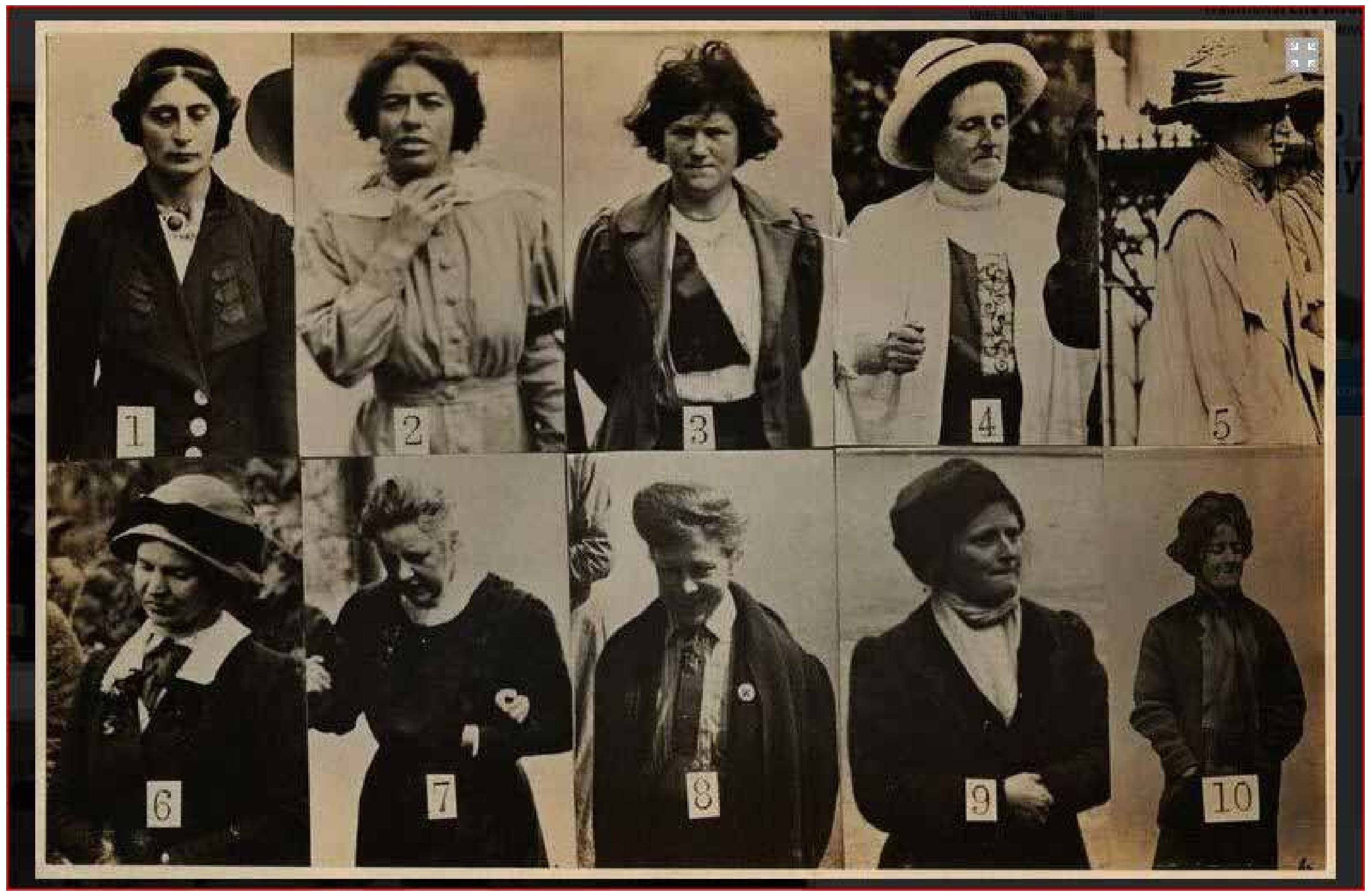
We would lose the opportunity to vastly expand access and distribution of independent news and community information through broadband television. More than 60% of Web content is created by regular people, not corporations. How will this innovation and production thrive if creators must seek permission from a cartel of network owners?

Most of the great innovators in the history of the Internet started out in their garages with great ideas and little capital. This is no accident. Network neutrality protections minimized control by the network owners, maximized competition and invited outsiders in to innovate. Net neutrality guaranteed a free and competitive market for Internet content. The benefits are extraordinary and undeniable.

Congress is deciding on the fate of the Internet. The question before it is simple: should the Internet be handed over to the handful of cable and telephone companies that control online access for 98% of the broadband market? People are waking up to what's at stake, and their voices are growing louder by the day. 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?

What would you do if you discover that your mobile handset records your location whereabouts without your knowledge? James Bridle chose to take control and recycle it into a book. In the process, he ends up assessing our status quo with digital memories.

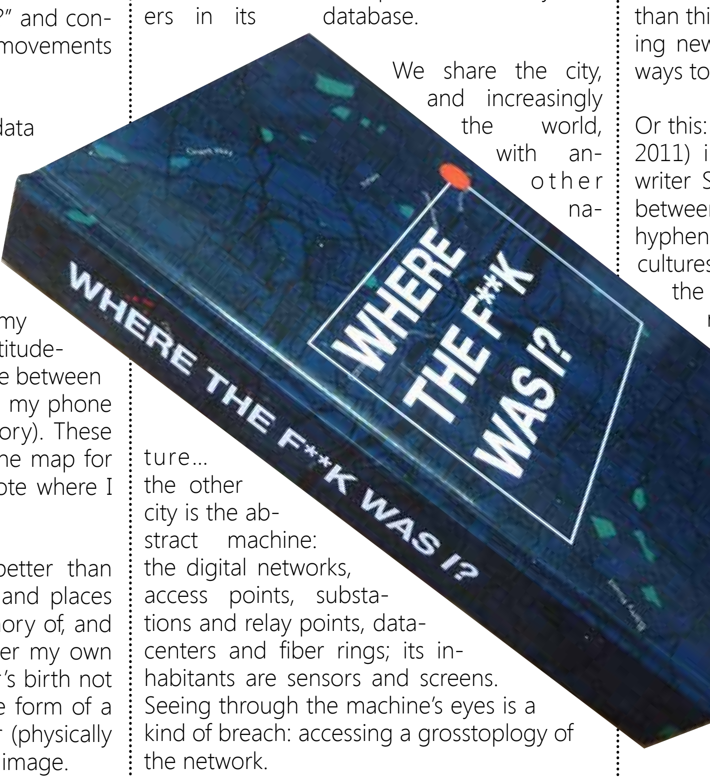
James Bridle

"I have 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 users' 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 have no personal, onboard memory of, and over time I come to rely on it over my own memories. Just as I recall my sister's birth not through my own vision, but in the form of a photograph of the event, I appear (physically and impossibly) in my own mental image.

This digital memory sits somewhere between experience and non-experience; it is also an approximation and a lie. These location records do not show where I was, but 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 nature… the other city is the abstract machine: the digital networks, access points, substations 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 grosstoplogy 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 astronauts 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? Carboncentric?).

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 so long, find a place in the world."

More at http://bit.ly/kVaNAF

Next Issue: Group Behavior Online.

Deadline: August 5.

Please send your contributions to:

nilofar.ansh@gmail.com

Let's Talk Open

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 pairs individuals and collective freedoms & 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 Fear In The Digital Age blogathon, I also voiced my fear about private corporations gaining 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 handout: a manifesto of sorts (see image below), 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 manifesto and needs 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 of future military developments?

It is also important to understand the effects on the overall information network that specific nodes 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 (and get away with). It may sound simple, but such a perceptual shift would be very helpful.

Person First

Consumer second

MY RIGHT TO INFORMATION WILL NOT BE RESTRICTED!

Steps to exercising your rights

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

NewsBytes

Perfect filtering of information on the internet will lead to a fractured communication environment http://bit.ly/q1RNlw

----

Andrew Keen: Compulsive sharing of everything through e-mail, Facebook, and Twitter is really a trap. The logical conclusion of all this personal diarrhea — Keen says "we are our own Wikileakers" — creates a frightening world in which private lives all but disappear.
http://ind.pn/9koCId

The (in)Visible Subject: Power, Privacy and Social Networking
by Rebecca Schild
Schild argues that the interplay between privacy and power on social network sites works ultimately to subject individuals to the gaze of others, or to alternatively render them invisible
http://bit.ly/ppAvib

Privacy, By Design
For me, the most interesting questions to come out of Saturday's open-space discussion of Privacy, By Design at CIS were those that focused around how the notion of 'privacy' is constructed and negotiated.
http://bit.ly/gZ01JO

What next for privacy?
"The internet is in part a marketplace for horrific images of violence and abuse. Should we say that, because these images are created and circulated via many different jurisdictions, we should do nothing about them — and allow them to be created and circulated here, too?"
http://bit.ly/jpgmnW

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 of the Internet, states should negotiate a framework convention on cyberspace.
http://bit.ly/kA8sVR

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, itExtreme and Webshield) have agreed to start censoring the internet, blocking a secret list of websites from view.
http://bit.ly/mGOwBq

Africa's First National Open Data Initiative:
Kenya becomes the first country in Africa to launch a national open data initiative.
http://whiteafrican.com/2011/07/07/africas-first-national-open-data-initiative-kenya/

Yahoo planning to spy on user's emails:
According to the new change in 'terms of conditions of use,' Yahoo will also be able to spy on incoming emails from individuals and businesses without prior permission or warning.
http://bit.ly/pjqFkn

Authorities urged to produce evidence that jailed blogger is alive and well
The Committee to Protect Journalists (CPJ) and the Arabic 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/syria/2011/06/24/jailed_blogger/

Does the internet inhibit democracy?
Video: http://www.youtube.com/watch?v=Uk8x3V-sUgU&feature=youtu.be
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, Rebecca MacKinnon describes the expanding struggle for freedom and control in cyberspace, and asks: How do we design the next phase of the Internet with accountability and freedom at its core, rather than control?
Video: http://bit.ly/oHx3YA

Guest Editor: Nilofar Ansher | Design: Albert Mucunguzi (http://almuc.me) / Ronald Muhwezi (@Arr_emRonnie)

http://www.cis-india.org/research/dn/2011/07/03/links-in-the-chain-call-for-participation

Big Brother's Watching

Government Agencies Withholding Information on Data-Gathering from Facebook, Twitter, and Other Online Communities

San Francisco - The Electronic Frontier Foundation (EFF), working with the Samuelson Law, Technology, and Public Policy Clinic at the University of California, Berkeley, School of Law (Samuelson Clinic), filed suit today against a half-dozen government agencies for refusing to disclose their policies for using social networking sites for investigations, data-collection, and surveillance.
http://bit.ly/phEiPe

Transparent Government, via Webcams in India

That is the premise for the webcam that a top government official - Oommen Chandy, the chief minister of Kerala state, in southern India - has installed in his office, as an anticorruption experiment. Goings-on in his chamber are viewable to the public, 24/7.

In an India beset by kickback scandals at the highest reaches of government, and where petty bribes at police stations and motor vehicle departments are often considered a matter of course, Oommen Chandy is making an online stand.
http://nyti.ms/ncn9u2

Video Surveillance and Its Impact on the Right to Privacy

The need for video surveillance has grown in this technologically driven era as a mode of law enforcement. Video Surveillance is very useful to governments and law enforcement to maintain social control, recognize and monitor threats, and prevent/investigate criminal activity. In this regard it is pertinent to highlight that not only are governments using this system, but residential communities in certain areas are also using this system to create a safer environment.
http://bit.ly/pWxiWB

Americans Soon Facing Harsh Penalties for Illegal Downloads

Text: After years of negotiations with Hollywood and the music industry, the nation's top Internet providers have agreed to a systematic approach to identifying customers suspected of digital copyright infringement and then alerting them via e-mail or other means. Under the new process, which was announced this July, several warnings would be issued, with progressively harsher consequences if the initial cautions were ignored.
http://bit.ly/nCIQw7

When Data Means Privacy, What Traces Are You Leaving Behind?

What does privacy really mean? In a society that is increasingly relying on information to identify people, collecting and archiving 'personal' details of your lives, your name, age, passport details, ration card number, call records etc, how private is your tweet, status update, text message or simply, your restaurant bill?
http://bit.ly/orHbu3

Whistleblower

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

In a recent interview, the Canadian Privacy Commissioner was quoted as saying "Information and the manipulation of information is the key to power. Those who can control the information can influence society enormously." History and present-day society have both proven the truth in this statement. It is one among many reasons that the right to information is important to uphold. 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, information that is publicly available.

An entirely separate but equally critical way in which the public is kept informed 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 information, whistle-blowing, and the right to privacy are 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 whistleblowing is supposed to be disclosure in 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 remedy or avoid actual wrongdoing rather than simply publishing 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. In many countries, a person may present information of a whistleblowing nature to a judicial body. The judicial body then determines the validity of the information, the degree of public interest involved, and the proper form of redress to be taken. The judicial body offers legal protection to the whistleblower. Another method of whistleblowing is to leak information to the press. Once information is in the public domain – at least if there is freedom of press -- the information can no longer be covered up. 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 as competent authority to deal with complaints file by whistleblowers and as the tribunal to protect whistleblowers. Structuring the power to allow one body to fulfil both functions runs the risk of bias and 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 do not want to leak their information to a judicial body or are not protected if they do so in their own country. Leaking information to Wikileaks is in one sense analogous to leaking information to the press, but it is not precisely the same because it is not a news media outlet, 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 immunity that individuals who leak to authorities are granted. When an individual shares documents or information with Wikileaks, the site in turn acts as a platform to publish 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 involved. Paul Chadwick, the Victorian Privacy Commissioner, pointed out that for the whistleblower the main privacy concerns include the individual's identity, safety and reputation. 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 jeopardized by disclosures. The Wikileaks saga squarely presents the question whether intent should be brought into the analysis of privacy and whistleblowers. If a whistleblower is disclosing with the intent to protect the public, the protections afforded to this person should weigh differently against the privacy interests of alleged wrongdoers and third parties than for someone who is simply defining the public interest as "interesting to the public," or, worse, is looking to leak information to disrupt public interest.

Even though Wikileaks works to protect the anonymity of individuals who leak information, it is not bound by any law to protect the privacy of individuals involved in the leak. The concept behind Wikileaks is important. By interacting with government information, it has the ability to bring accountability and transparency to governments, 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 could place individuals in precarious situations or damage reputations with no validating information.

Read the original post here: http://bit.ly/hYUmVK

Is Pakistan putting the UN Millennium Goals at risk?

With the 2011 Internet Governance Forum (IGF) slated for a September run this year, **Nighat Dad** *looks back at the forum in Vilinius, Lithuania last year where she argued for a proactive UN engagement with women & youth in the area of Internet regulation to fully realize the MDG3.*

The IGF is an international body, set up by the United Nations (UN) to address global issues of governance in the online world. It was instituted five years ago and is linked to the UN's Millennium Development Goals, of which Millennium Development Goal 3 (MDG3i) is specifically concerned with the evolution of women's rights.

The IGF as an inclusive forum

The discussions I witnessed at IGF 2010 really brought home the scale of challenges we still face. For instance, although the Internet has been with us for a decade-and-a-half, no one can seriously claim that government regulations concerning cyberspace does enough to combat violence against women in the cyber world. The technology may have evolved at a phenomenal pace, but social, cultural and legal changes proceed at a far slower pace. And yet, the time stipulated to achieve the MDG3 is just five years!

A national perspective

While the discussions and initiatives at IGF are welcome, I challenge whether they are enough, in the absence of serious national debate – particularly in developing countries like Pakistan, where such discourse remains extremely rare.

There is mounting evidence that Pakistani girls and women are victims of cyber crimes, including cyber stalking, cyber pornography and cyber bullying. I see a certain irony in our interactions with web technology. While on one hand we have quickly adapted to online services like YouTube, Facebook, mobile SMS as well as MMS (multimedia messaging service), we have also easily – and readily – learnt how to use these platforms for subversive intents. The situation is especially acute for young women and children who have no training or exposure to cyber crimes and unwittingly fall prey to criminal actions.

What is not often understood, even in supposedly inclusive and well-informed communities like the IGF, is the appalling impact these actions can have, particularly in developing nations with more restrictive or conservative cultures. What might, in some Western nations, amount to no more than an immature but harmless prank, can – in countries like Pakistan, have the most dire results: a homemade, manipulated video of a young Pakistani girl, uploaded and disseminated online, can cause untold harm to the subject, who may find herself facing subsequent loss of personal liberty, mobility and recreation, and even deprived of educational, employment and marital opportunities, leading to social boycott and parental censure.

The legal dimension

I freely admit: these are complex social and cultural issues, and neither technology nor law alone can offer a solution. However, it seems to me that one sure way to fail is to try and address them in the absence of legal protections against cyber crime.

Pakistan's own 'Prevention of Electronic Crime Ordinance 2007' was allowed to lapse several months earlier, and there is no sign of new legislation being brought forward. Unfortunately, in absence of cyber law, only one remedy is available under Section 509 of the Pakistan Penal Code, which allows victims to register complaints against harassment through the Police Enforcement Authority.

The enforcement authority which deals with cyber crime (the Federal Investigation Authority, or FIA) says there is no law in the country at the moment to check cyber crimes, and as a result they are unable to take action on any cyber-crime related complaints.

A call to action for the UN

On 16 September 2010, the UN Secretary-General Ban Ki-moon launched the 2010 MDG Gap Task Force Report with the following words: "Tremendous progress has been made in strengthening (international) partnerships but the agreed deadline of 2015 is fast approaching and there is still much to be done".

Mr Secretary General, for all the progress you mention towards stronger international partnerships, I hope this report makes it clear that in some respects, we are actually worse off now than we were a little under two years ago, in November 2009. Our government shows little interest in giving its citizens either legal protection, or practical guidance on how to protect themselves.

The deadline for MDG3 is not just challengingly close: it is seriously at risk. If member states such as Pakistan are allowed to do nothing, the UN cannot meet its Millennium Development Goals.

As the chief sponsor of the IGF and the Millennium Development Goals, please send the following message to the governments of Pakistan and other developing nations:

- Act now, to engage stakeholders such as the women and the young; don't allow their valuable input to be lost through inaction on your part;
- Act now, to establish the right legal framework within which your citizens' rights can be protected against malicious and criminal online activity;
- Act now, to make the internet a safer place, where your culture and society can thrive, evolving in pace with technology, not threatened by it.

But above all, act.

Read the original post here: http://www.genderit.org/feminist-talk/pakistan-putting-un-millennium-goals-risk

What Open Data Means to Marginalized Communities

Joshua Goldstein

Two symbols of this era of open data are President Obama's Open Governance Initiative, a directive that has led agencies to post their results online and open up data sets, and Ushahidi, a tool for crowd-sourcing crisis information. While these tools are bringing openness to governance and crisis response respectively, I believe we have yet to find a good answer to the question: what does open data means for the long-term social and economic development of poor and marginalized communities?

I came to Nairobi on a hunch. The hunch was that a small digital mapping experiment taking place in the Kibera slum would matter deeply, both for Kiberans who want to improve their community, and for practitioners keen to use technology to bring the voiceless into a conversation about how resources are allocated on their behalf.

So far I haven't been disappointed. Map Kibera, an effort to create the first publicly available map of Kibera, is the brainchild of Mikel Maron, a technologist and Open Street Map founder, and Erica Hagen, a new media and development expert, and is driven by a group of 13 intrepid mappers from the Kibera community. In partnership with SODNET (an incredible local technology for social change group), Phase I was the creation of the initial map layer on Open Street Map (see Mikel's recent presentation at Where 2.0). Phase II, with the generous support of UNICEF, will focus on making the map useful for even the most marginalized groups, particularly young girls and young women, within the Kibera community.

What we have in mind is quite simple: add massive amounts of data to the map around 3 categories (health services, public safety/vulnerability and informal education) then experiment with ways to increase awareness and the ability to advocate for better service provision. The resulting toolbox, which will involve no tech (drawing on printed maps), and tech (SMS reporting, Ushahidi and new media creation) will help us collectively answer questions about how open data itself, and the narration of such data through citizen media and face-to-face conversations, can help even the most marginalized transform their communities.

We hope the methodology we develop, which will be captured on our wiki, can be incorporated into other communities around Kenya, and to places like Haiti, where it is critical to enable Haitians to own their own vision of a renewed nation.

Read the original post here

http://bit.ly/cycHp1 Joshua Goldstein is a technology policy PhD candidate at Princeton University's Woodrow Wilson School, where he works with the Center for Information Technology Policy. He is also on the Board of the Ugandan software consultancy Appfrica Labs and has worked extensively in East Africa.

He blogs at http://bit.ly/rhmsVH |
Twitter: @african_minute

Guest Editor: Nilofar Ansher | Design: Albert Mucunguzi (http://almuc.me) / Ronald Muhwezi (@Arr_emRonnie)

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 assertive of back home in Egypt, but never really expressed while traveling. Now that I live in South Africa, 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 me into a loud, incessant and boring voice. Being alienated from my blog is making things worse, as I only 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 "The Dispossessed" 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 anarchist human society, living with no government, power hierarchies or private property.

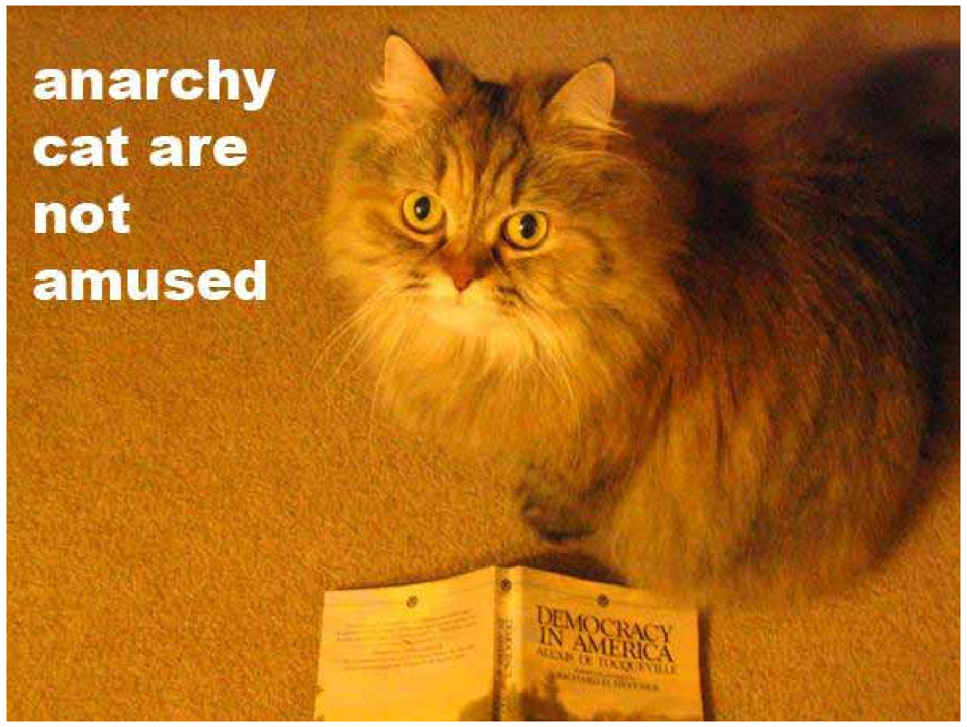
Dispossession

In Ursula's novel, dispossession is a positive thing and a choice. But I also chose the word because it can be understood in many ways and carries negative connotations as well.

I'm a reluctant anarchist: I don't buy any of the narratives that justify states, borders, capital or governments; I abhor power in all its forms and totally distrust representative democracy. And yet, I live within modern society. I consume. I have a career. I engage in politics as they are (and I enjoy these activities). I find myself very able to imagine the world Ursula describes (and even see (and live) glimpses of it in spaces as diverse as slums, free software movements and youth camps.

While I am unable to imagine a move from how we are today to a state of dispossession - if it can happen - I have no patience for people who cannot imagine anarchy. People, who are not only comfortable with the status quo (of semi, quasi democracy), but cannot bring themselves to imagine other possibilities (of un-governance).

Part of the reasons why I chose to live in South Africa is to do with the romantic notion that I will be living among a victorious people. As Arabs, we are resigned to a very pessimistic view of the future; history and politics are a long list of defeats; my personal short history as an activist is full of optimism, but entirely made of defeats; I thought living in post-Apartheid South Africa would teach me and inspire me. Instead, what I found is a very right wing, conformist society. I met the fiercest defenders of the status quo. Not a day passes when I don't feel that Egypt, with all its despair and decay, is a much more dynamic and free society (than South Africa).



It was with joy that I participated in the word-matching activity at the Digital Native workshop because it provided me with the chance to see how an understanding of my reluctant anarchy is shared with participants from different political backdrops and frameworks of viewing democracy.

> **"I don't buy any of the narratives that justify states, borders, capital or governments; I abhor power in all its forms"**

Restoration

Khanyile from Zimbabwe chose restoration to symbolize the need for Zimbabweans to restore their sense of power, their control over their destinies and livelihoods. We first discussed how power is always within the people. All power is derived from the masses but we seem to need to relearn 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.

Passion and Hope

Evelyn from Uganda chose passion. To her, passion is what drives one to try and change the world. Marlon from South Africa chose hope. He works with the dispossessed (in the very traditional sense); some have been dispossessed even of a place in society (being members of gangs or sex workers), but it is hope that they've truly been dispossessed of, and it is hope that they need to regain control of their lives.

I found it interesting that such basic human traits like passion and hope need to be relearned. I guess that's what we need to reaffirm our power. Loss of passion or hope can be a state that befalls anyone; even those who live in harsh environments can find hope and passion. Possession and dispossession in their positive and negative aspects are functions of the imagination.

And activism is at its essence a practice in mythology. 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 it brought tears to my eyes that such a document 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 living 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 abhor?

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 essentially 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/a5pTpk

Accolade for McSpeedy

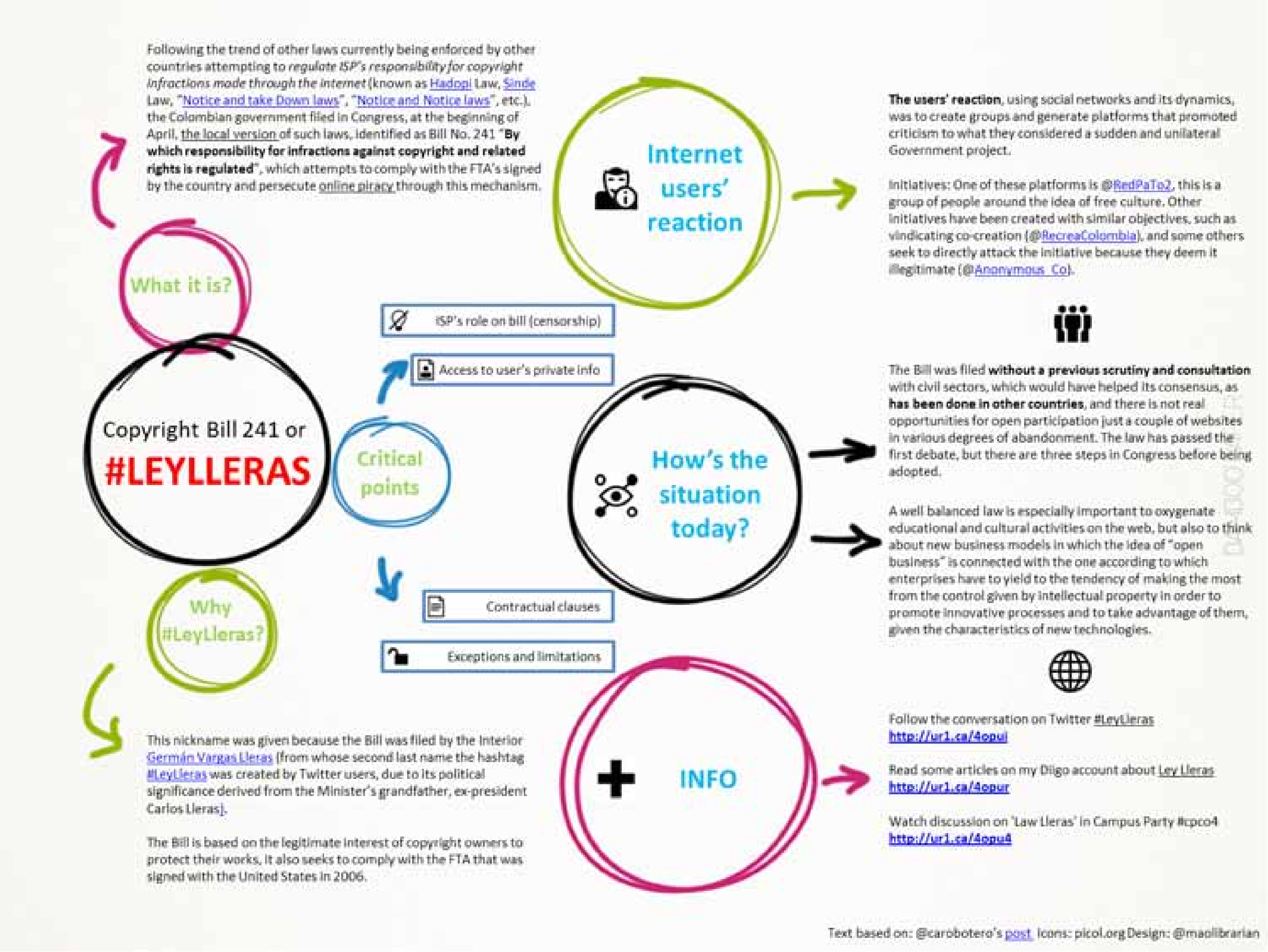
Written in the Hindi language by Indian poet **Pradeep Madhok,** the poem bids a fond farewell to McSpeedy, the courier pigeon.

एक चट्िठी अपने पहचान वाले को लखि रहा हूँ
कुछ पुरानी यादें फेर ताज़ा कर रहा हूँ
एक वक़्त था जब संदेशो वाले कबूतर उसके घर
भेजा करता था
कबूतर का नाम मुस्सदि रखा था मैने
मुस्सदि कभी इस मुंडेर पे कभी उस मुंडेर पे बैठ
जाया करता था
मैं डरता था कि कोई संदेशा खो ना जाए
बरस के बादल कच्ची स्याही धो ना जाए
लेकनि हर बार उसका जवाब आता था
हर बार अपनी दुआओं पे यकीन आता था..
वो कबूतर समझते थे मेरी चाहत शायद
भाँप लेते थे बंद लफिाफे से मोहब्बत शायद
आज भी याद है मुझे वो मुस्सदि अपना
पैग़ाम ला के उसका छत पे गुटरगूं करना
पर अब वो मासूम डाकयिा कहीं खो सा गया है
अब e-mail ही सबका मुस्सदि हो गया है
आज का कबूतर Facebook, Google और Twitter
हो गया है
अब भी वो कभी इस मुंडेर, कभी उस मुंडेर रुका करते
हैं
हाँ मगर अब संदेशे ज़रा जल्दी पहुचते हैं..
पहले बारशि से डरता था, अब लफिाफे मे virus का
ख़ौफ़ होता है
तब कलम घसिा करता था, आज उंगलयिा घसिता
हून लखिने मे
ये भी मुशसादी की तरह भारी संदेशे ले के उड़ नही
पाता
लेकनि ये मुशसादी की तरह लखिने वाले की खुशबू,
स्याही नही लाता
बस मुस्सदि चट्िठयिा खोल के पढ़ता नही था
कसिी संदेशे को ले जाने पे अकड़ता नही था
मेरे लखिे शब्दो पे कभी सवाल नही कयिा उसने
मेरी पहचान पे कभी कोई बवाल नही कयिा उसने
बस इसी रशि्ते भर की दोस्ती थी अपनी
मैं लखिा करता था वो सुना आता था..

As I write a letter to someone familiar,
I refresh memories that are old & unclear
There used to be letter carriers,
Of the winged varieties
that flocked together
This one particular pigeon, I called him
McSpeedy, the winged deliverer of letters
Twittering here, settling there, chirping
of stories from everywhere.
Fear would strike me not unlike,
the thunderous clouds with lightning strikes,
Perhaps their tear drops would wash away
The words inked on paper, as pliable as clay.
But my prayers have never gone unanswered
With every flight, McSpeedy brought answers
He understood my yearnings unspoken
The love letters bound us together.
He flits in my mind, McSpeedy and his flight
Now he's best remembered as legacy,
The hearty messenger with wings
For email s have buried McSpeedy,
I write on the pages of Facebook, Google &
Twitter Inc.
The e-McSpeedy is no different
He follows in the footsteps of his antecedent
And moves around with upgradable options!
But the fear no longer is about speed
I lie awake thinking of the need
Of spies to pry open my mail
Rain no longer dampens my parade
It's those evil viruses that put me naked
For they know not the scent of a page
They know of only filter & damage.
These private letters from me to you
Would never be read by any but you
For McSpeedy had eyes only on target
He nv'r questioned what he was told to
forget.
It is this friendship I remember today
For McSpeedy I write in praise,
Let me end my email here
The Draft folder is now clear.

Colombia's Copyright Bill 241

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



Following the trend of other laws currently being enforced by other countries attempting to *regulate ISP's responsibility for copyright infractions made through the internet* (known as Hadopi Law, Sinde Law, "Notice and take Down laws", "Notice and Notice laws", etc.), the Colombian government filed in Congress, at the beginning of April, the local version of such laws, identified as Bill No. 241 "**By which responsibility for infractions against copyright and related rights is regulated**", which attempts to comply with the FTA's signed by the country and persecute online piracy through this mechanism.

This nickname was given because the Bill was filed by the Interior Germán Vargas Lleras (from whose second last name the hashtag #LeyLleras was created by Twitter users, due to its political significance derived from the Minister's grandfather, ex-president Carlos Lleras).

The Bill is based on the legitimate interest of copyright owners to protect their works, it also seeks to comply with the FTA that was signed with the United States in 2006.

The users' reaction, using social networks and its dynamics, was to create groups and generate platforms that promoted criticism to what they considered a sudden and unilateral Government project.

Initiatives: One of these platforms is @RedPaTo2, this is a group of people around the idea of free culture. Other Initiatives have been created with similar objectives, such as vindicating co-creation (@RecreaColombia), and some others seek to directly attack the initiative because they deem it illegitimate (@Anonymous_Co).

The Bill was filed **without a previous scrutiny and consultation** with civil sectors, which would have helped its consensus, as **has been done in other countries**, and there is not real opportunities for open participation just a couple of websites in various degrees of abandonment. The law has passed the first debate, but there are three steps in Congress before being adopted.

A well balanced law is especially important to oxygenate educational and cultural activities on the web, but also to think about new business models in which the idea of "open business" is connected with the one according to which enterprises have to yield to the tendency of making the most from the control given by intellectual property in order to promote innovative processes and to take advantage of them, given the characteristics of new technologies.

Follow the conversation on Twitter #LeyLleras
http://ur1.ca/4opui

Read some articles on my Diigo account about Ley Lleras
http://ur1.ca/4opur

Watch discussion on 'Law Lleras' in Campus Party #cpco4
http://ur1.ca/4opu4

Text based on: @carobotero's post. Icons: picol.org Design: @maolibrarian

Limits to Privacy

*When does the right to information supersede the right to privacy? **Prashant Iyengar** talks about privacy of online communication within the framework of the Indian IT Act of 2008*

The legal alibis that the State employs to justify its infringement of our privacy are numerous, and range from 'public interest to 'security of the state to the 'maintenance of law and order'. In this paper, I attempt to build a catalog of these various justifications, without attempting to be exhaustive, with the objective of arriving at a rough taxonomy of such frequently invoked terms. In addition I also examine some the more important justifications such as 'public interest' and 'security of the state' that have been invoked in statutes and upheld by courts to deprive persons of their privacy.

Article 12 of the Universal Declaration of Human Rights (1948) refers to privacy in the following terms: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Similarly Article 17 of the International Covenant of Civil and Political Rights (to which India is a party) declares that: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home and correspondence, nor to unlawful attacks on his honor and reputation."

Communications laws

All laws dealing with mediums of inter-personal communication – post, telegraph and telephony and email – contain similarly worded provisions permitting interception under specified conditions. Thus, Section 26 of the India Post Office Act 1898 confers powers of interception of postal articles for the "public good". According to this section, this power may be invoked "On the occurrence of any public emergency, or in the interest of the public safety or tranquility". The section further clarifies that "a certificate from the State or

Central Government" would be conclusive proof as to the existence of a public emergency or interest of public safety or tranquility.

Most recently, Section 69 of the Information Technology Act 2008 (India) contains a more expanded power of interception which may be exercised "when they [the authorized

officers] are satisfied that it is necessary or expedient" to do so in the interest of

a) Sovereignty or integrity of India,

b) Defense of India,

c) Security of the State,

d) Friendly relations with foreign States or

e) Public order or

f) Preventing incitement to the commission of any cognizable offence relating to above or

g) For investigation of any offence,

From a plain reading of these sections, there appears to be a gradual loosening of standards from the Post Office Act to the latest Information Technology Act. The Post Office Act requires the existence of a 'state of public emergency' or a 'threat to public safety and tranquility' as a precursor to the exercise of the power of interception. This requirement is continued in the Telegraph Act with the addition of a few more conditions, such as expediency in the interests of sovereignty etc. Under the most recent IT Act, the requirement of a public emergency or a threat to public safety is dispensed with entirely – here, the Government may intercept merely if it feels it 'necessary or expedient'.

How much of a difference does it make?

Excerpts from the research paper Limits to Privacy. The full version can be downloaded here: http://cis-india.org/advocacy/igov/limits-privacy.pdf/

MAKE QUOTATION Symbol in the center of this article – in a box: "When does public interest supersede the right to privacy?"

How to Promote Net Freedom? Simple, Support Cyber Anarchy!

Simeon Oriko rants against the 'hackivist' groups online who rip apart legitimate and legal cyber platforms under the guise of digital activism and free culture.

The last few months have been really eventful for net users and digital activists and for me in particular. There has been increasing chatter concerning net freedom and I'm genuinely concerned about the repercussions of our efforts to keep the web open and self-regulated.

Take for example the recent wave of cyber attacks. Two "hacktivist" groups, LulzSec and Anonymous, went about defacing websites, hacking servers and illegally obtaining user credentials online. While their actions are rooted in a cause, the means to achieve this end is cruel and has caused suffering and embarrassment to the victims.

Take for example one Aaron Barr, former CEO of HBGary Federal, a US-based cyberspace security firm. Barr had found himself at the center of a scandal that began when he told the Financial Times of his plans to reveal the names of some "leaders" of the hacker group Anonymous.

When members of Anonymous discovered Barr had been involved in the investigation, they engaged in an intense counter-attack, wiping his iPad along with its backup storage, and copying large amounts of work-related email messages from him. This data was later shared on the Internet via a peer-to-peer file sharing service. They also took over his Twitter account, published his social security number, remotely wiped his iPhone, exposed his World of Warcraft character name(s), and revealed personal details from his life.

It gets interesting. Forbes reports: "Anonymous...exposed a darker side to HBGary Federal's business that offered a variety of dirty tricks to its clients. In a proposal intended for Bank of America_and written on behalf of a law firm referred to the bank by the U.S. Department of Justice, Barr suggested borderline illegal tactics that aimed at responding to a potential release of the bank's documents by Wikileaks. Those methods included cyber attacks, misinformation, forged documents, pressuring donors and even blackmailing Wikileaks supporter and Salon journalist Glenn Greenwald. In another deal, HBGary suggested a similarly shady response to the Chamber of Commerce in its campaign against the Chamber's political opponents including non-profit organizations and unions."

> **"Worse, these actions have triggered a cyber warfare that includes stealing data, defacing websites and Denial of Service Attacks, all of which go against the principles of Internet Freedom"**

Naturally, this embarrassed Barr, his clients and the U.S government...but that's the lesser part of the damage. Both the actions of Anonymous and Barr have far reaching effects beyond the scope of their individual groups/organizations. The actions possibly put millions of users at risk of having their digital identities unmasked and their privacy ripped apart for other cyber utopians to "lol" about (as in the case of hacker group LulzSec). Ironically, Barr fell on the same path of the axe he had set out to attack the groups with.

Worse, these actions have triggered a cyber warfare that includes stealing data, defacing websites and Denial of Service Attacks, all of which go against the principles of Internet Freedom.

So what exactly are we doing? Destroying the moral and ethical fabric of the digital world? Supporting a cause by bringing down other legitimate structures? Championing anarchy for the sake of Internet Freedom? Yeah, right!

In the name of fairness

*The common man needs safeguards from cyber crimes while having his freedom of expression protected online. **Diego Caseas** makes a case for limited government regulations.*

When I was asked to write about Internet Governance and Online Regulation, I immediately accepted, because this is one topic that most activists of freedom of expression are actively engaged with through debates, policy or implementation. We want to make sure that the Internet is not regulated into a place where basic human rights are violated, or where control over access and the user's activities online are monitored by the government.

I guess what drives people into fighting for a free and open Internet is the fear that people's voices are not going to be taken into account in the decision-making process. We do not know if our representatives will defend the position of the user/citizen, or rather the interests of ISPs. And that is why it is so important to bring this debate to many areas of social life, be it in schools, universities, at your work place or private spaces.

This discussion is the same everywhere, with little change from country to country. In Brazil, our major problem is the Digital Crimes Bill. It is still proceeding, and it is intended to be voted very soon (protests of the hacker groups LulzSec and Anonymous have caused a stir inside the Congress), but what this bill does is typify common practices such as cyber crimes, punishing users with restrictive sanctions and even arrests. What it does is ignore all public-civil discussions about the subject and the new practices that have emerged with the use of the Web.

To make sure that net users' concerns are addressed, the Ministry of Justice has made initiated a public hearing, collecting ideas and opinions from citizens, promoting discussion on the subject and calling on citizens to help shape the bill. The Marco Civil is intended to be voted in the Congress, and when this happens, many rights such as anonymity and privacy, safety and security, will be considered. This will go a long way in protecting human rights defenders and allowing free speech on the Web.

When it comes to regulating the Internet, there are two types of legislation: one that will punish the user and benefit ISPs and Intellectual Property agencies, on the excuse that they want to promote the market and the liability of the service; the other way is ensuring that at least the bare minimum of opinions from users are heard, and that basic human rights are considered as pillars of this regulation. If we don't do so, we risk being used as puppets in the hands of private companies and governments.

It smells like coffee in here, *at least for now*

***James Mlambo** cautions us to take systematic action against excessive government cyber regulation - or face a future without flavoured coffee beans.*

The issue of Internet regulation is bittersweet for me. If I fall victim to identity theft and the culprits are brought to book by government agencies, then I am all for letting the government regulate the Net. But, if a blogger is thrown into filthy police cells for simply posting blogs that are critical of the government – all in the name of internet regulation - then I certainly won't stand for government control of cyberspace.

Why are calls to regulate the Internet growing loud these days? The first people to drink coffee did so under no one's regulations. But when coffee started spreading across the breadth and length of the world, an endless list of players ranging from researchers, traders, capitalists and industrialists jumped in to regulate coffee. Before we know it, demonstrators are up in arms against the police at the WTO meetings over coffee grievances. No wonder why our grandmas are saying today's coffee no longer taste and smell the same as the ones produced earlier.

In the same vein, if the current discourse on internet regulation is not handled systematically, then a couple of years into the future we will have a case of netizens complaining about the net 'losing its flavour'. I find it funny to imagine that decades later, we might have digital activists standing alongside coffee growers and consumers at the WTO, demanding the return of their original flavours for drinking - and surfing!

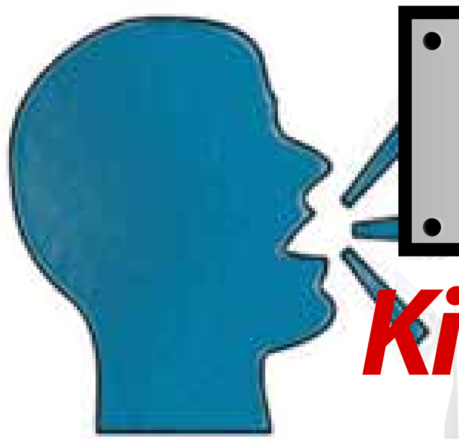
The Internet is still young, less than 20 years old. In many African countries, it is less than a decade old. Zimbabwe is currently emerging from a decade-long economic meltdown the highlight of which was a world record inflation rate of 13.5 billion percent. Infrastructure development or rehabilitation of the telecom sector as well as providing web technology training and services to consumers supersedes the need to regulate or take control over users' activities online.

If the US congress had thrown Mark Elliot Zuckerberg an internet red book, I don't think he could have come up with Facebook (and the same applies to other web app developers). Governments in developing countries should leave students and youths to experiment with their ideas without much regulation. We want our African university and college campuses to produce Afro-centric solutions and platforms for furthering development in our continent. For that to happen, the current criticism of Internet regulation needs to persist. If changes are to be made, then it must only be deregulation of already existing rules that are stifling internet development.

Internet regulation can be visualized in capitalist democracies, where dissent is possible – in case government tightens the strings too much – and also receives institutionalized support. In oppressive African states, the idea of internet regulation will be used as an excuse by dictators to abuse, suppress and victimize people – bloggers, political commentaries, critics, media and citizen journalists and activists.

Isn't it time to let the Internet graduate, from maybe its adolescent stage to adulthood? Haven't we listened to the other voices shouting "Let the Internet self-regulate"? As soon as this Internet baby made its first birth cry across several African nations, we are in a hurry to strangle its voice. Do we ever think of 'regulating' a baby? Do we 'govern' a child, or guide it, is the tough question that both the government and citizens need to discuss.

Guest Editor: Nilofar Ansher | Design: Albert Mucunguzi (http://almuc.me) / Ronald Muhwezi (@Arr_emRonnie)



NO SILENCE PLEASE

Killing the Internet Softly with Its Rules

While regulation of the Internet is a necessity, the Department of IT, through recent Rules under the IT Act, is guilty of over-regulation. This over-regulation is not only a bad idea, but is unconstitutional, and gravely endangers freedom of speech and privacy online, says ***Pranesh Prakash***

Regulation of the Internet, as with regulation of any medium of speech and commerce, is a balancing act. 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. This is especially so with the Internet, as it has managed to be the impressively vibrant space it is due to a careful choice 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), the safeguards that cyber cafes need to follow 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, or communication link made available or hosted. It qualifies that by stating that they are not liable if they follow certain precautions (basically, to show that they are real intermediaries). They observe 'due diligence' and don't exercise an editorial role; they don't help or induce commission of the unlawful act; and upon receiving 'actual knowledge', or on being duly notified by the appropriate authority, the intermediary takes steps towards some kind of action.

So, rules were needed to clarify what 'due diligence' 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 Act 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 YouTube, to organizations and people that allow others to post comments on their website. What kinds of terms of service? It will require intermediaries to bar users from engaging in speech that is disparaging'. It doesn't cover only intermediaries that are public-facing. So this means that your forwarding a joke via e-mail, which "belongs to another person and to which the user does not have any right" will be deemed to be in violation of the new rules. While gambling (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. Any 'affected person' can complain. 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 of 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 cardinal principle of natural justice of 'hearing the other party' before denying them a fundamental right. Many parts of the Internet are in fact public spaces and constitute an online public sphere. A law requiring private parties to curb speech in such a public sphere is unconstitutional insofar as it doesn't fall within Art.19(2) of the Constitution.

Since intermediaries would lose protection from the law if they don't take down content, they have no incentives to uphold freedom of speech of their users. They instead have been provided incentives to take down all content about which they receive complaints without bothering to apply their minds and coming to an actual conclusion that the content violates the rules.

Given that all of these were pointed out by both civil society organizations, news media, and industry bodies, when the draft rules were released, it smacks of governmental high-handedness that almost none of the changes suggested by the public have been incorporated in the final rules.

Read the full post here: http://bit.ly/ntieHw

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 unreasonable and — given the multitude of online voices — poorly thought out, says ***Anja Kovacs***

In March 2011, Indian media - both social and traditional - was ablaze with fears 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 Due Dilligence 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 block 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, instances of vigilante groups destroying art, preventing film screenings, or even attacking offending artists, writers and editors have become noteworthy for their regularity. But it is worth noting that even more progressive sections of society have not been averse to censorship: for example, section of the Indian feminist movement have voiced strong support for the Indecent Representation of Women Act that seeks to censor images of women which are derogatory, denigrating or likely to corrupt public morality.

What connects all these efforts? A belief that suppressing speech and opinions makes it possible to contain the conflicts that emanate from India's tremendous diversity, while simultaneously ensuring its homogenous moral as much as political development. But if the advent of satellite television already revealed the vulnerabilities of this strategy, the Internet has made clear that in the long term, it is simply untenable. It is not just that the authors of a speech act may not be residents of India; it is that everybody can now become an author, infinitely multiplying the number of expressions that are produced each year and that thus could come within 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 mostly continued on the beaten track, putting into place a range of legislations and policies to meticulously monitor and police the freedom of expression of netizens within its borders. Thus, for example, section 66F(1)(B) of the IT (Amendment) Act 2008 defines "cyberterrorism" so broadly as to include the unauthorised access to information on a computer with a belief that that information may be used to cause injury to...decency or morality. The suggested sentence may extend to imprisonment for life.

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, constraining the Internet access of crores of young people among the less advantaged sections of society in particular. And while the US and other Western countries continue to debate the desireability 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 Internet brings for freedom of expression everywhere, 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.

Read the original version here: http://bit.ly/fLIrgt

Alt / Tab

The Next Step Towards an Open Internet

How about a Federal Friendship Commission — an offshoot of the Federal Communications Commission to regulate social networks and 'friendships'?

Joshua Kroll

Now that the FCC has finally acted to safeguard network neutrality, the time has come to take the next step toward creating a level playing field on the rest of the Information Superhighway. Network neutrality rules are designed to ensure that large telecommunications companies do not squelch free speech and online innovation. However, it is increasingly evident that broadband companies are not the only threat to the open Internet. In short, federal regulators need to act now to safeguard social network neutrality.

The time to examine this issue could not be better. Facebook is the dominant social network in countries other than Brazil, where everybody uses Friendster or something. Facebook has achieved near-monopoly status in the social networking market. It now dominates the web, permeating all aspects of the information landscape. More than 2.5 million websites have integrated with Facebook. Indeed, there is evidence that people are turning to social networks instead of faceless search engines for many types of queries.

Social networks will soon be the primary gatekeepers standing between average Internet users and the web's promise of information utopia. But can we trust them with this new-found power? Friends are unlikely to be an unbiased or complete source of information on most topics, creating silos of ignorance among the disparate components of the social graph. Meanwhile, social networks will have the power to make or break Internet businesses built atop the enormous quantity of referral traffic they will be able to generate. What will become of these businesses when friendships and tastes change? For example, there is recent evidence that social networks are hastening the decline of the music industry by promoting unknown artists who provide their music and streaming videos for free.

Social network usage patterns reflect deep divisions of race and class. Unregulated social networks could rapidly become virtual gated communities, with users cut off from others who could provide them with a diversity of perspectives. Right now, there's no regulation of the immense decision-influencing power that friends have, and there are no measures in place to ensure that friends provide a neutral and balanced set of viewpoints. Fortunately, policy-makers have a rare opportunity to pre-empt the dangerous consequences of leaving this new technology to develop unchecked.

The time has come to create a Federal Friendship Commission to ensure that the immense power of social networks is not abused. For example, social network users who have their friend requests denied currently have no legal recourse. Users should have the option to appeal friend rejections to the FFC to verify that they don't violate social network neutrality. Unregulated social networks will give many users a distorted view of the world dominated by the partisan, religious, and cultural prejudices of their immediate neighbors in the social graph. The FFC can correct this by requiring social networks to give equal time to any biased wall post.

However, others have suggested lighter-touch regulation, simply requiring each person to have friends of many races, religions, and political persuasions. Still others have suggested allowing information harms to be remedied through direct litigation—perhaps via tort reform that recognizes a new private right of action against violations of the "duty to friend." As social networking software will soon be found throughout all aspects of society, urgent intervention is needed to forestall "The Tyranny of The Farmville."

Of course, social network neutrality is just one of the policy tools regulators should use to ensure a level playing field. For example, the Department of Justice may need to more aggressively employ its antitrust powers to combat the recent dangerous concentration of social networking market share on popular micro-blogging services. But enacting formal social network neutrality rules is an important first step towards a more open web.

Joshua Kroll is a graduate student from the Department of Computer Science, Princeton University. He blogs at Freedom to Tinker.

The original post appears here http://bit.ly/pPgpZ0 and was written on April 1 on All Fool's Day

Read more on FCC and net neutrality here: http://bit.ly/diQ3j6 & http://bit.ly/i47eWc

Guest Editor: Nilofar Ansher | Design: Albert Mucunguzi (http://almuc.me) / Ronald Muhwezi (@Arr_emRonnie)

REGULUS REGULATORE v/s ANNA ANARCHICA

Maria del Mar Zavala

Whenever I come upon an article or a debate on internet governance, I always find myself torn. While I tend to lean more towards a liberalized Internet—without any restrictions—I do think that some sort of regulation is necessary at some level, so as to provide individual users, companies and even states with protection.

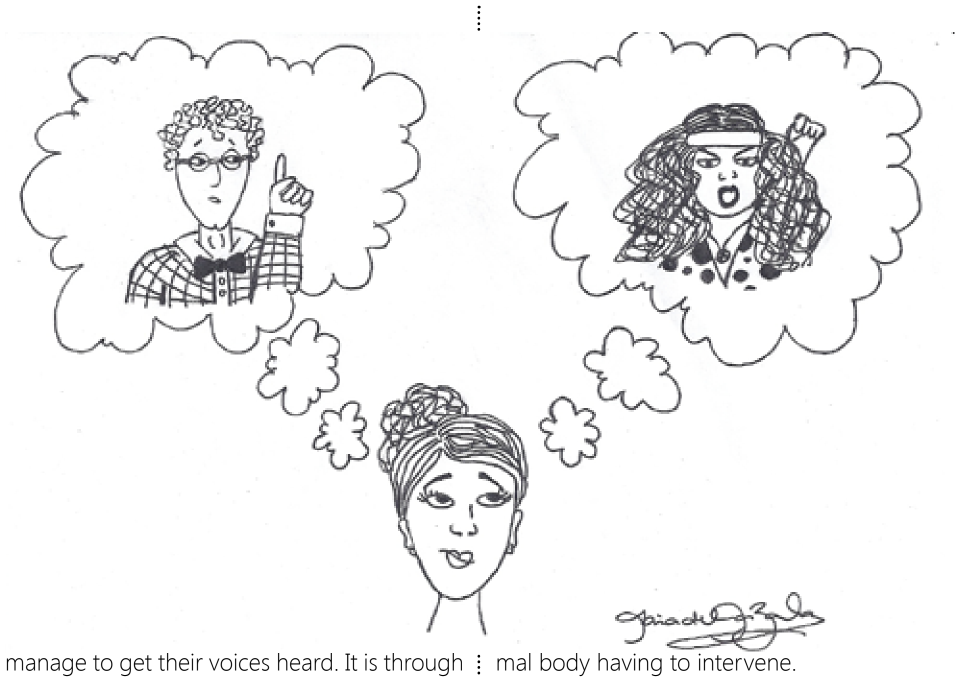
It is a complicated issue, and whenever I think about it, it is as if I have two people with completely different points of view arguing in my head. It is sort of like when in cartoons, you see the little angel and little devil popping up on each side of the hero/ine's head, telling him/her what to do. Only that in my head, instead of having the little angel and devil, I have Regulus Regulatore and Anna Anarchica urging me to pick their side. Here goes their chatter:

Anna Anarchica: Seriously, Maria del Mar? You are even considering supporting limiting freedom? That is not what you stand for! You dedicate your work to freedom of access to information and freedom of speech!

Regulus Regulatore: Anna, why are you being so melodramatic? Maria doesn't want to limit freedom, she just wants a bit of control.

Anna Anarchica: Control??!!! So, are we cheering for Big Brother now?

Regulus Regulatore: Hey! People need to be responsible for their actions online. Right now, anyone can do whatever they want, and it is not only the good guys who are using the Internet after all! It is a total free-for-all!



Anna Anarchica: Keyword being "free"! It is by means of the Internet that the oppressed manage to get their voices heard. It is through the Internet that people can share their views and opinions!

Regulus Regulatore: But it is also through the Internet that companies and governments get hacked...and cyber bullies attack!

Anna Anarchica: The pros far outweigh the cons.

Regulus Regulatore: What about creating an international body for Internet dispute resolution? That has proven to be efficient for international agreements in other areas of governance, policy and regulation.

Anna Anarchica: I don't believe that is necessary. Things will eventually settle without a formal body having to intervene.

Regulus Regulatore: Anna, that is not how things work. If there is no formal internationally-agreed system in place, then the stronger party will always be at an advantage. Don't you think that this is a good reason for creating an international regulatory body dedicated solely to net management?

Anna Anarchica: No, Regulus, I don't. I believe in laissez-faire...

And the debate between Anna Anarchica and Regulus Regulatore goes on and on... They both raise very important points, but I can never decide whom to side with. How about you? Are you more of an Anna or a Regulus?

Poetry in Motion

A tale-in-verse of gastronomic mishaps, retold by **Hasina Hasan.**

The parts of a poem
were so constructed
by four co-authors
while being seated,
in diverse global locations
with their hearts-n-minds-unitedly-working,
to the socially just cause
of a simple affirmation...
of L.I.F.E.
So, on to an FB status message they piled,
line after line,
in spritely synchronocity.
Below the Panda's status message,
the Piggy posted a comment,
the little Ladybug another,
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 poe-m!

But | but | but | but | but | erm,
the piggy butted in
"POST PRODUCTION"
Piggy said, "Give it to me now!"
POST PRODUCTION
Piggy nearly caused a little pow-wow
POST PRODUCTION.

Only then did they realise,
they didn't know The Law
To whom could the verses cling,
Who governed it all?

((((Oink)))) ((((Oink)))) ((((Oink))))
The piggy couldn't just wait
She rushed to her lawyer
Mr Lorrie, who was an expert
in these lyrical matters.

Mister Lorry spoke at length:
"Now you see that words of joint co-authorship need to be co-jointly intended by the authors who intended to co-write firstly on a joint platform. Yes. Also note that individual contribution should be indistinguishable from group distinguishing characteristics. Post partum, do be ...."

Phew! Sighed the piggy,
Ears ringing with music,
the lyrics of Mr Lorrie
was intestinally manic *_*
Piggy didn't wait to hear the rest
Piggy huffed and Piggy did fret
Piggy rushed from Mr. Lorry, P,
Bee & Bug
Not for a moment realising
that it was just
A simple case of stomachly upset
Yes THAT'S RIGHT!
Piggy had a case of indigestion.

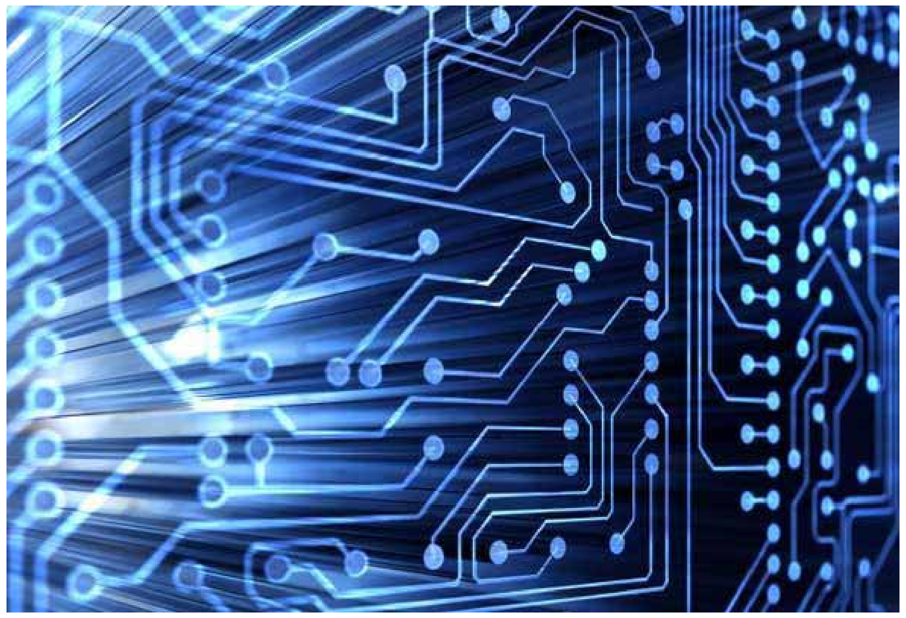
Back home, Piggy to the Bee
Rattled subversive cacophony
When all she need have done
was take a simple colon test
Ooh, Aah, Ouch clucked
Piggy with crackling poo
Pained Piggy / looking silly
in her irritable bowel distress.

Guest Editor: Nilofar Ansher | Design: Albert Mucunguzi (http://almuc.me) / Ronald Muhwezi (@Arr_emRonnie)

Of Politically Agnostic Technologies

The politics of design, of interface and the potentials of exclusion and discrimination that are built into the very structure of technology are often overlooked or made invisible, says Nishant Shah.

I often wear multiple hats **(sometimes one on the top of the other – like Dobby in the Harry Potter books)** in my interactions with digital and internet technology – amateur coder, information architect, Web 2.0 user, cybercultures researcher, technology enthusiast... the list is longer than one would have imagined. In recycling myself through these various roles, there is one thing that has often worried me, especially when I talk to many who use these technologies for making change – and it is this inherent belief that technologies are disconnected from politics. Let me dwell on this for a bit **(or a byte, if you will).**



The debates around whether the rise and spread of decentralized, digital easy to access technologies have proven to be a catalyst for social change and political participation is fraught with partisan positions. On the one hand are people who celebrate the negotiation and intervention making power of these technologies and attribute to them great agential power that can change the world. On the other are those who look at these tech developments with great suspicion, trying to make a case for the power of the human will rather than the scope of technology design. On either side of the Technology line, the arguments rage, fast and furious, and often futile. While they see a cause-and-effect link between technology and politics – technology as a tool in the hands of those demanding and making change, there is a deafening silence around the idea of **Political Technologies.**

The functional focus on digital technologies – economic prosperity, time-space shrinkage, transparent interaction and governance – has been so overwhelming that in the realm of the WWW, technologies are imagined as agnostic to politics; more scarily, for me, there seems to be this established disconnect between the everyday practices of technology and the spectrum of politics within which we operate. Let me give a hypothetical **(and hence the absolute truth; as opposed to factual)** analogue example to explain this further.

Take a blank sheet of paper, for example. To all appearances, the blank sheet of paper, is completely agnostic to the uses it can be put to. It can become a letter of love, drenched in overpowering affections, it can be a note of dismissal shattering dreams for somebody who is fired, it can be a financial promissory note facilitating complex legal and economic transactions, or it can become the rag you use to mop a spill on your desk. It is generally presumed, that the piece of paper does not really have any design or agency that will change the world forever. And yet, for anybody studying the history of technology, it is obvious that this sheet of paper did indeed revolutionise and change the world. The advent of the printing press, the ability to mass-produce paper, the possibility of sending disembodied messages and communications, the power of the paper to store information which can then be retrieved, has been transforming the world the last five hundred years. It is a technology – print or writing – that, by its very design possibilities and limitations, is able to shape, not only how we have communicated with each other, but also how we think of ourselves. Let us remember that the first proof of our identity, is not in images or in sounds but in a document, printed on a piece of paper, that declares us human and alive and legally present – the birth certificate.

I take the example of the blank sheet of paper, because we have grown so use to the world of letters, of writing and of printing that we have appropriated paper as an integral part of the human socio-cultural fabric. However, it is necessary to realize that technology interfaces and products have not only a political agenda in their design, but also the power to shape the ways in which human history and memory function. That the blank sheet of paper, in its inability to capture oral traditions, eradicates them. The tyranny of a piece of paper makes invisible the ways by which human articulation is recorded and fixed, instead of allowing it the negotiation power that fluidity brings with it. The conventions of writing, the processes of reading, the very technologies by which print products are produced, are determined by the material, formal, efficient and final design and potentials of this interface. To think of the paper as bereft of political design, ambition and destiny, would be to neglect the lessons learned in human history.

The digital interface **(and the surrounding paraphernalia of tools and apps**) is right now facing a similar problem. There is, in the seductive nature of the interface, a value of agnosticism which allows for the proliferation of these digital interfaces. It is presumed that the digital interface – home for so many of us – in itself is not political in nature. In fact, it is so in the realm of the cultural and the everyday that its design and application does not have any political charge. This disavowal of political ambition and intervention on the part of digital technologies is something that scares me. It makes opaque not only the more obvious political economies of digital technologies – who owns them? Who supports them? Who pays for them? Who benefits from them? Who controls and regulates them? Who remains excluded? Who is being made to bear the burdens? More significantly, **it reduces all politics to the level of content –** so that we constantly get new 'readings' of the data streams that they generate.

In all these questions, **the politics of design, of interface and the potentials of exclusion and discrimination which are built into the very structure of technology** are often overlooked or made invisible.

- How do technologies determine who gets a voice?
- How do the digital webs exclude those who shall always remain outcasts?
- What are the kind of people who get to become digital natives?
- What happens to our understanding of the relationship between the state and the citizen?
- What are our digital rights?
- How does the technology design and structure mitigate social evils?
- How does technology emerge as the de-facto arbitrator of law?

In its very presence, technology is political. Politics play a part not only in the tool-based approach (remix-share-reuse) but in the very nature and rise of the digital technologies. To think of them, in the postmodern fashion, as a-political, as agnostic to politics, as without an ideological mooring, and as disconnected from the everyday personal politics, is something that scares me... because it lets people believe that they can interact with technologies without worrying about the often contradictory and generally tyrannical structures of being that it produces. It makes others believe that digital natives, hence, can be located entirely in the realm of lifestyle shopping and cultural consumption and not to be reckoned as actors of political change and transformation.

Like the feminists of old, it is time perhaps to proclaim that like the personal, the "The Technological is the Political"

Nishant Shah is Director (Research) at the Centre for Internet & Society, Bangalore
http://bit.ly/o2ggqm