Southern African Internet Governance Forum

Issue Papers[1]
No. 3 of 5

Security, Openness and Privacy

Produced by the Association for Progressive Communications (APC) in partnership with SANGONeT. Written by Alex Comninos.

Table of contents

1. Introduction

This is the third paper in a series of papers prepared for the Southern African Internet Governance (SAIGF) forum that serve as an introduction to the themes to be discussed at the 6th Annual Internet Governance Forum in Nairobi 2011. The papers are structured to reflect the themes of the IGF, which correlate with plenary sessions and related feeder workshops. These papers are intended to provide an introduction to the possible issues to be discussed at the IGF and to stimulate debate during the IGF. The papers raise more questions than they answer and are not intended to inform policy recommendations or provide detailed analysis of any of the issues to be discussed at the IGF.

What are the most significant Internet Governance Issues that affect security, openness and privacy? According to the Draft Programme for the Nairobi IGF:

"Current examples for discussion are (but not limited to): The role of "new media" / "citizen journalism" and the roles of new media, journalism and citizens' media. Actions taken by a range of Internet actors, in relation to whistle-blower sites - including the the "seizure of" of domain names. The growing importance of information security. Proposals for blocking websites and

---

filtering of networks, and the impacts of action taken to cut access to the Internet for individuals, groups, or entire countries from the global Internet."[2]

Questions suggested in the programme are:

- "What are the most significant cross-border Internet governance issues that affect security, privacy and openness? What is the role of traditional and new media, journalist and citizen journalist in the Internet 3.0 world?

- Is the ability to read over the Internet essential in a democratic society? What are the implications for Internet governance when online censorship is imposed by the private sector (e.g. a web hosting provider) and not the government? Is it a violation of human rights to cut Internet access that individuals, specific groups or entire countries rely on?

- What are the implications of those actions for online freedom of expression, assembly and association?

- Is the content distribution and communication capacity that the Internet affords important to fostering human rights?" Should we identify self-regulatory policies, regulatory choices and best practices for players in the Internet ecosystem that protect openness, privacy, and security for all individuals?"[3]

At the SAIGF, the topic will be addressed in two separate sessions: one dealing with cybersecurity and the other dealing with cross-border Internet Governance issues such as regulation, intermediary liability and freedom of expression.

Additional questions to be asked are:

- How should we regulate the internet? How should we protect children and vulnerable persons from access to unsafe content? What are the various levels and loci of responsibility – parent, service provider and the state?

- How do we deal with freedom of expression versus content control?

- Can the internet be censored? Should the internet be censored?[4]

The session will build upon last year's Security, Openness and Privacy main session on the role intermediaries to protect freedom of expression and innovation.

Possible issues are discussed below which include the role of the new media, whistle-blower websites, the effects of censoring websites, information security issues as well as new issues relating to privacy and anonymity on social networks. These issues are introduces to stimulate

---

[2] Internet Governance Forum, Draft Programme for the 2011 Meeting, 09 August 2011, intgovforum.org/cms/2011/programmepapers/ProgrammePaper2011.Aug%209.doc

[3] Ibid.

[4] Background Paper for the Southern Africa Internet Governance Forum.

debate about possible issues that may be discussed at the IGF. The issues contained in this paper are just suggestion for discussion at the Southern African IGF and the IGF, but do not reflect particular debates at either forum.[5]

The role of new media / social media / citizen journalism

New media - media created and shared in new ways over the internet (such as blogs, video and picture sharing, podcasts, micro-blogging and social networking) -, has and is having affect on how we consume news about the world around us.

Some call it "new media". Some people call this phenomenon "user-generated content" because it is generated by users of the internet or of content creation devices (like computers and mobile phones) rather than by professionals and corporations. Some call it "citizen journalism" because it enables anyone (with ICT access) to report on events and act as a "journalist". It can be also called "social media" because it involves media that is easily shared/communicated/disseminated often in a social manner (e.g. on social networks like Facebook). Social media implies of also that others who do not create the content can be active in its dissemination, aggregation (collecting) and curation (choosing for publication / dissemination) of content. As indicated by the diagram below, this is a complex ecosystem, and understanding new media, does not entail just understanding how content is created and consumed, but involves a basic understanding of the current state of the internet content ecosystem.

Figure 1. The content ecosystem[6]
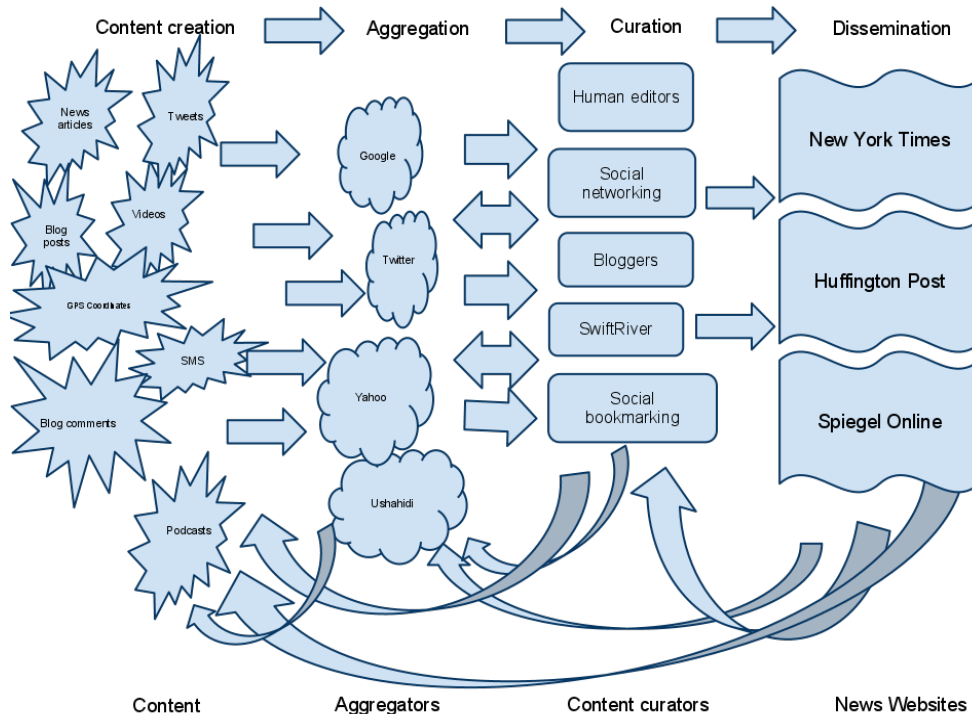
Content consumers are increasingly turning to new media when following news events. When access is blocked to journalists, or journalists cannot be somewhere for security or whatever reasons the mobile phone often becomes a tool for recording events and social media for sharing and disseminating this news. This has provided windows on much protest action and state response, as well as on conflicts that much of the world may not see if it were not for new media. Old media is becoming increasingly reliant on new media in covering events. Journalists are increasingly using this user-generated content and information from social networking websites to inform media consumers.

These new ecosystems for content creation, aggregation and distribution are outlined briefly in the diagram above, which should to be taken not as a rigid typology or model, but rather as a suggestion for discussion, and possible modification. The convergence of new and old media on the whole has been of enormous benefit for consumers of the media, as well as for transparency and openness within societies.

What is the role of journalist in a "Internet 3.0" world where social networking and user-generated content are prevalent both as a platform and a source of news and information? New media can also be a tool of misinformation (as can old media). Misinformation can spread quickly over new media. Remember the "lesbian blogger" who "disappeared" in Syria? This turned out to be a heterosexual American man. Remember the few dozen times (over a variety of media) we had heard that Moammar or Saif Ghadafi had been captured, when it turned out not to be the case?

When disinformation is spread through the media, it often spread by both old media as well as by new media. When misinformation is spread it is often through the whole content ecosystem, and many actors in both the old and new media are complicit, whether they consciously spread it or not. New media can help to also "crowd-source" analysis and commentary on new media stories and can thus contribute to a media consumers ability to find different opinions on sources they may come across?

2. Action taken by internet actors in relation to whistle-blower sites

2011 may be remembered as the year of torrential downfall of information leaks, including many state and corporate secrets. Julian Assange has been quoted as saying "courage is contagious". Journalists and bloggers have had much "courage" this year in analysing and citing the trove of US embassy cables which continue to be released at a rapid rate (35 000 new cables were released on 23 August). Whistle-blower sites like WikiLeaks and Crytpome, although an age-old internet practice which were not that popular with internet users, except a small number of activists, bloggers, journalists and geeks, are now proliferating. New whistle-blower sites are constantly emerging.

While some may feel that whistle-blower sites are a threat to national or corporate information security, others feel that such sites can have a role in making the actions of governments transparent to citizens, and thus possibly stimulating good governance and accountability.

Do whistle-blowing and leaks sites present particular challenges to internet governance? Which whistle-blowing sites are permitted by states and other internet governance actors and which are

not? Whilst some leaks can serve a whistle-blowing purpose, other leaks can serve to dump huge troves of information online, often including personal data.

Should states be able to censor whistle-blowing websites? And under what conditions should they do so? And under what conditions is leaked information to be considered legal public domain information and under which is it not? If censorship approaches are taken, which data would be censored, and in whose interest would that be? States? Companies? Netizens? or Citizens? What would be the implications of these actions for the media and journalism? What would be the implications of these actions for transparency, accountability and anti-corruption initiatives?

Taking whistle-blower websites down, or blocking access to them is not particularly effective, as their content can be mirrored throughout the web faster than it is removed, filtered or blocked. Whistle-blowing, or leaking, of course need not happen on on sites dedicated to that particular purpose. Leaked information need not of course even be spread on conventional web infrastructure. Often leaks are spread through torrents (peer to peer file sharing) or posted on Facebook or Twitter.

3. The effects of censoring websites

If websites are taken down, there can usually be "collateral damage" - that is others that had nothing to do with the offending sites can be indirectly affected. Most small websites on the internet exist on shared hosting, that is, a number of websites use the same computer as a web host, and can share the same IP address, if punitive action is taken by one website, be it through flooding the website (like for example with Distributed Denial of of Service attacks), through the hacking of the website, or through action taken against its Domain Name Servers (DNS), or the blocking of IP addresses, many other websites sharing the same infrastructure can be affected.

After actions against WikiLeaks' domain name servers in 2010[7] mirrors of WikiLeaks (copies of the content of WikiLeaks) continued to grow from from a rather small amount of mirrors to hundreds, and then thousands of mirrors on domains and IP addresses all across the internet. This has been referred to as the "Barbara Streisand Effect", whereby suppressing information/media has the unintended consequences of stimulating the proliferation of that very media/information.[8]

In August 2011, action (equivalent to a subpoena) was taken again against WikiLeaks' DNS server. Will the actions described above be set to repeat themselves?

As pointed out above, whistle-blowing and leaking can happen on a variety of platforms, if websites are closed down, leaks can still be posted on social networks, they can continue to be shared via peer-to-peer networks or on "hidden parts" of the web such as onion (Tor) websites. Cracking down on whistle-blowing websites could thus have the effect of growing covert communication networks also known as "Dark Nets"[9], as well as forcing content into the hidden sections of the

---

[7] For a description see: Charles Arthur and Josh Halliday, WikiLeaks fights to stay online after US company withdraws domain name, The Guardian, 03 December 2010, guardian.co.uk/media/blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns.

[8] For a legal perspective on this effect see: David Corneil, The Streisand Effect, WikiLeaks, and Social Media, americanbar.org/content/dam/aba/events/communications_law/200504_24_the_streisand_effect_wikileaks_and_socia_media.authcheckdam.pdf

internet, only used Thus such actions could have a negative effect on an open and transparent internet.

Once leak sites have gone into the public domain, how are sites that mirror their information or bits of information considered by internet governance actors. Can sites be considered worthy of censorship for mirroring for using data that is already in the public domain? Taking censorship, and well as punitive action against whistle-blowing and leak sites can thus have adverse and often negative effect on journalism. Considering the degree by which leaks mirror themselves over the internet, are cited and analysed and written about, censoring leaks would involve massive scale censorship, and a suppression of free speech.

4. The increasing importance of information security

Whilst leaks and whistle-blowing sites can be both forces for openness and transparency, they can also be damaging to states, corporations as well as citizens to which the information refers to or affects.

States using internet governance to restrict or regulate leaking need to consider not just action taken against leak-sites but also information security policies within states, corporations, and regulatory institutions. Some have worried that wave of reported hacking attacks in 2011, represent the emergence of an "information security" apocalypse. As one Information Security practitioner stated referring to the large proliferation of data security breaches recently, and why some in the information security industry were glad about these developments - "there is an elephant in the room".[10] Information security issues and vulnerabilities that have been known for some time, and for which there are solutions, often go ignored. These these are becoming real information security risks. Despite information breaches, the information security sector and the general public are becoming increasingly aware of information security risks. A positive effect of the events described above could be that corporations, states and the general citizenry revise their information security policies and implementations for the greater benefit of all stakeholders, including the privacy of individuals.

Those that have been the victim of leaks, or data breaches, regardless of the effect of these breaches (positive or negative) also need to assume responsibility for the fact that the data was breached in the first place. Whilst it has yet to be proven who was responsible for the leaking of the US Embassy cables, it has been suggested that for the person accused it was as easy as copying the contents of files and saving the to files to a rewritable DVD (whilst pretending to listen to Lady Gaga). It is worth remembering that "More than 3 million US government personnel and soldiers, many extremely junior, are cleared to have potential access to this material".[11]

---

[9] Darknets are not neccessarily for distribution of illegal or covert content, for example much open access academic and learning material, as well as linux distributions are distibuted via torret. See Wikipedia contributors, Darknet (file sharing), http://en.wikipedia.org/wiki/Darknet_(file_sharing) An article by four Microsoft employers defines a darknet as " The darknet is not a separate physical network but an application and protocol layer riding on existing networks. Examples of darknets are peer-to-peer file sharing, CD and DVD copying, and key or password sharing on email and newsgroups." Peter Biddle, Paul England, Marcus Peinado, and Bryan Williamson (Microsoft Corporation), 2002, http://msl1.mit.edu/ESD10/docs/darknet5.pdf.

[10] Patrick Gray - Risky Business (podcast), Risky.biz/LulzSec.

A large degree of breached and leaked data in 2011 was acquired through very simple tools exploiting vulnerabilities that are well known in the security industry. Security researchers have reported on and provided solutions to these vulnerabilities years ago, but these have not been widely implemented. This could be due to a reluctance to spend money on data security due to other budgetary constraints, but it more importantly could be a capacity and knowledge problem. There are many cheap (and also many open source) solutions to avoid these problems.

The focus on leaking and whistle-blowing at the IGF should not be disproportionately focused on the "leakers". The information security community, and stakeholders at the IGF reliant on information security to protect their data, should also be compelled to keep their own house in order, as a means of preventing data breaches, and protecting people whose data they are entrusted with.

We should be mindful that these extra-ordinary measures do not infringe on privacy and openness. When states invest in cybersecurity they may be investing in both offensive and defensive measures. Defensive measures should take precedence in state and corporations, in order to both focus on the security of information, as well as to avoid the militarisation of cyberspace.

5. New issues: Privacy on social networking websites

Privacy involves the right to selectively reveal information about oneself, and to chose whom to reveal the information to. Thus if data has been posted on a social networking website (with certain levels of access restrictions to certain persons) that data is still private, and social networking websites should respect and protect that privacy. In addition to collecting the information we provide them, social networking websites can collect extra information (our location, the things that we are interested in etc.) that we have not expressly allowed (or we may have expressly allowed for this but not read the terms and conditions). Data can be shared by social networking websites (as well) as by search engines and given to third parties, usually advertisers, who may then even in turn pass this data on to others. This is not a conventional area of internet governance, especially at the national and regional level. Social networking websites are only under the regulatory and policy domains of the servers in which they are hosted, and users, regardless of in which country the user signed the same terms and conditions.

The state of Schleswig-Hollstein in Germany has recently proposed a ban on the use of the Facebook "like" button on websites in Germany. This was not a ban on all "liking on Facebook" within the state of Schleswig-Holstein but rather of the application that allows for the Like button to be embedded in a particular site, so that the user may thus, "like" a page without going to Facebook. The reason for this, is that the use of the button (for example on state websites, or company websites within the German state), makes available information about the user and her browsing to Facebook and possibly third parties. It is understandable why the government of Schleswig-Holstein would not want to facilitate the sharing of its citizens' information (and possible breaches on their privacy) in this way. It is obvious that there would be different legal, policy and regulatory environments regarding the collecting storing and sharing of databases of private

---

[11] David Leigh, US Embassy Cables Leak Sparks Diplomatic Crisis *The Guardian* 28 November 2010, accessible, http://www.guardian.co.uk/world/2010/nov/28/us-embassy-cvs able-leak-diplomacy-crisis

information in the US, where Facebook is listed as a company, and a large amount of its servers are hosted; and the State of Schleswig-Holstein.

Should the regulation of cross-border sharing of databases of personal information be an issue brought onto the table at the SAIGF?

6. New issues: Anonymity on the internet

A long-running and revealing joke, emanating from a comic strip in the 1990s, was that "on the internet, nobody knows that you are a dog". This was of course a reference to the fact that on the internet, one could assume a anonymous, or "pseudonymous" identity by using a nickname instead of one's real name. This is a practice of course done for many different reasons, but one of the reasons was that the internet facilitated communications and communications with strangers in a way like never before (like for on example forums or message boards, Internet Relay Chat, image sharing platforms, Multi User Role Playing Games, etc...), and many people did not use their real name to protect themselves from any harm (virtual or physical) that would be inflicted upon them by internet users. Of course there is no real way for the average user to be anonymous on the internet, and they can often have their IP address, connection information and location revealed on the internet, anonymity afforded a small but important degree of protection and comfort to many internet users, and still does.

Enter Facebook, a horde of other social networking sites, and now Google Plus. These sites from their launch required users to give their real name, email address and often phone numbers. It is in the terms of conditions of Facebook, Google Plus and many other that a users real name must be given. Of course there were many who call themselves by monikers on Facebook. However Facebook, and more particularly Google's new "Plus" service, have recently been shutting down user profiles not conforming with real name policy, and there seems to be an argument both in the industry and in the policy community against anonymity. Randy Zuckerberg, at the time Marketing Director of Facebook stated that "anonymity on the Internet has to go away". This is neither possible, nor desirable, especially for those under repressive regimes. What extra-ordinary measures, like censorship and invasion of privacy would such an enormous feat entail?

Many influential online identities have been unmasked and linked to real identities during the Arab revolutions. Despite being detrimental to the people behind these identities, this unmasking can prove to be beneficial to the movements they supported. Google executive Wael Ghonim called for protests in Egypt with the use of an online moniker and was detained by the security forces. His public appearance on television after his release (and subsequent television appearance) mobilised many new protesters to take part in the protests, and the day after his release saw one of the biggest crowds ever at Tahrir Square. However those revealed as participating in protests online have also been unlucky disappearing in places like Egypt, and losing jobs in Bahrain for example.

Online identities provide opportunities for interventions by those external to the conflict and can often be harmful and counter-productive, as was the case of the Syrian "lesbian" blogger, who was revealed to be a non-Syrian heterosexual male. This supplied the Syrian government with "evidence" of foreign intervention in its affairs through the internet.

Fake online identities, or "sock-puppets" are not only used by non-state actors in information conflicts but are also increasingly used by states and military, security and intelligence agencies. Emails from US defence contractor HBGary which were acquired by hackers from Anonymous and leaked online reveal an "astro-turfing" software commissioned by the US Air Force. Astro-turfing refers to the practice of using multiple sock-puppets to mimic the activities of grass-roots movements online.[12]

---

[12]Peter Bright, Anonymous speaks: the inside story of the HBGary hack, ars technica, 15 February 2011, http://arst.ch/o9q; George Monbiot, The need to protect the internet from 'astroturfing' grows ever more urgent, The Guardian, 23 February, www.guardian.co.uk/environment/georgemonbiot/2011/feb/23/need-to-protect-internet-from-astroturfing.