INTERNATIONAL **HUMAN RIGHTS FUNDERS** GROUP

SEMI-ANNUAL CONFERENCE
NEW YORK CITY
JULY 13-14, 2010

Human Rights in the Digital Age: Mobilizing Freedom, Repressing Dissent

Tuesday, July 13, 2010, 9:30-12:00 pm

Facilitator:
Andrew **Puddhephatt, Sigrid Rausing Trust; Global Partners and Associates**

Panelists:
Chuck Cosson, Microsoft Corporation;
Thomas Hughes, International Media Support; Media Frontiers
Elisa Massimino, Human Rights First
Brett Solomon, Access

Sponsor:
Global Partners and Associates

Andrew Puddhephatt opened by explaining that the purpose of this morning's session is to illuminate the relevance of digital advances to human rights activism and human rights funders: what are the opportunities and the threats posed, and what are the values that we should advocate in the new digital world? The session will:

- Survey of the world of global technology
- Explore policy issues and collaboration between digital advancement work and human rights

He played a short video titled “Getting Past the Barbed Wireless” to introduce the importance of digital communication to human rights issues.

- One to many (traditional) versus and peer to peer (new media) communication networks
    - Digital ecosystem is less hierarchical and predictable; influenced by governments, businesses, technologies, users; empowers users to make positive use of technology.
    - E.g. Facebook, tool for US students, five years later tool to fight repression in Iran.
- Modes of communication are newly important because the platform can impact the content (censorship, security, dissemination) in the way that old communication technology could not.
    - We need to apply human rights standards and values not only to content but also to all technology infrastructure and policies.

Brett Solomon began by recounting that when he recently heard that an activist in Iran had been arrested, the first action they took was to secure her Gmail account for fear she would be tortured for her password, which would give the regime access to her conversations, documents, and address book. After the protests in Iran, a cat and mouse game ensued between the government and activists, with the regime trying to shut down/infiltrate the internet and various sites. Many of the people in Access worked with people in Iran to ensure that the images they took would be liberated. He played a video showing images of violence during protests to demonstrate the extraordinary power of citizen media and mobile phones: for example in China, there are currently 800 million mobile phones, which represents an existential threat to a repressive regime.

There is a whole process that is necessary to get citizen media out, but it can have a major impact. They’ve had almost 5 million views of some of the videos that they have been able to post to Youtube. Many of the people that they work with are not online right now, but a few years ago many of us didn’t even have mobile phones. It’s important to plan for 10-20 years down the road, for when access to technology has spread. Human rights activism increasingly relies on an open and unmonitored internet. E.g., in a recent election in Macedonia, it was possible to determine the outcome of the election in advance by the relative sizes of the candidate’s Facebook groups; there’s a potential for much greater, more widespread accountability in election monitoring through mass of individuals with mobile phones.

Iran is a canary in a coal mine since it has a particularly tech savvy and active population. Already 30% of the world lives behind a firewall (political, social, or conflict filtering). The human rights community is thus in need of digital relief, to allow people to access the digital sphere. The internet is a last resort when newspapers, radio, and TV have been cut off. Tools to circumvent blocks can get videos out – which can end up on CNN within hours.

In China, there are now more bloggers and online journalists than print journalists in prison, and they just commemorated the one year anniversary of the first blogger who died in prison. Bloggers are also at risk from attacks on their sites. A website is like a shopfront, and governments and hackers are closing those shopfronts down. It’s important to protect sites so that they stay online, and to secure connected items like email addresses and accounts.

Another issue is cyber warfare: the human rights community has traditionally played an important role in war, but what about cyber war? How is the human rights community prepared for these situations?

Even in Australia, now, the government is trying to establish a mandatory filter for child pornography – but this may set up a dangerous filtering system (China's state officials have reported on this effort positively). It is better to deal with it like printed materials; with police enforcement, not built-in censorship.

Decisions that we make now will impact the freedom and human rights of generations to come.

Q: In Iran, the use of a picture of the wrong person led to abuses of this other woman's rights.
A: There are many issues with ensuring accuracy of information acquired in a viral way (CNN at first refused to show citizen media). But steps can be taken such as filming the newspaper and your location for authentication. In traditional media, good gatekeepers can put in place ethical codes, but they cannot be sustained in the digital world. We need to collectively mature in our literacy and ability to interpret new media formats, as cultural literacy had to mature after the printing press.

Thomas Hughes noted that there's a lot of mythology about what technology can achieve – a "just add internet" philosophy that thinks technology will just automatically change the world. He wants to challenge and examine this, look at the ways that technology may help mobilize freedom but also be used to attack organization, and give examples of where digital technology has been used very well.

He plays a short clip of "The Satirical Donkey," made by the leaders of youth groups in Azerbaijan. It's gotten 110,000 views and has been broadcast on the BBC, but the two men who made it were attacked and badly beaten, then arrested and imprisoned for 2 and 2 ½ years. An online petition was made to protest this, but attention has dropped, the organizations have lost funds and membership, and the government has posted material online to smear the activists' reputations – so who won out?

Big assumptions about technology and reasons to doubt them:

- Digital communications reinforce participatory governance and undermine authoritarian regimes
    - But: "digital natives" may be more focused on the virtual world than the real world; technology does not equal transparency; you can access information without technology.
- Digital communications empower democracy by giving voice to all
    - But: narrow information scope (only get the information you seek); diminished role of journalism and standards; empowers politically motivated groups.
- Digital communications act as a multiplier to mass movements during crisis
    - But: movements are not necessarily sustainable or created by technology; unclear whether online tools are used more domestically in diaspora (Iran vs. Kyrgyzstan)
- Digital communications facilitate pro-democratic civil society activities
    - But: governments are often better at making use of them than civil society is

Areas of government control over digital communications:

- Policy and regulation: for defamation, anti-terrorism, national security, and pornography; growing to include copyright, intellectual property, e-governance, access to information, outlet registration, declaration of income, cyber-crime, blasphemy, and information sovereignty

- Monitoring and surveillance: everything is subject to interception (phones, email accounts, sites)
- Technical interference – blocking and filtering, shaping (making loading slow), attacks (taking over computers to crash websites), cloaking (to access information) and event-based control (e.g., closing down networks during demonstrations or elections).
- Counter Propaganda – flooded content (drowning out opposition), targeted content (putting own content on forum), slander, deceptive content to create illusion of transparency

Case study: Burma
He shows a video from Mizzima, an independent exiled Burmese media agency, discussing the challenges getting information into and out of Burma, harsh sentencing of Burmese journalists, and the use of state media to discredit other local and international media. Citizens are eager for outside information, and are becoming more and more experienced as citizen media and VJs. Mizzima workers have daily communications with reporters in Burma through internet proxy servers and mobile phones, and use security such as encryption to protect their communications. Democratic Voice of Burma broadcasts independent media 24 hours a day by satellite, the government has been unable to stop citizens within the country from smuggling in satellite dishes.

Q: What efforts are being made to counteract government propaganda efforts, and can activists only act on the defensive?
A: Thomas Hughes answers that in general that's true, but there are a few examples of opportunities activists took advantage of, such as the brief window when security controls were down after the cyclone in Burma. Brett Solomon agrees, and says that his organization is defensive, but they do counterblock IP addresses that attack them, for example. One reason to frame ourselves in defensive terms is to avoid starting an arms race.

Andrew Puddhephatt discusses the prominent role of social networking platforms. These are all business applications developed by large companies, and the companies themselves often play a central role in the digital battles for human rights. He introduces **Elisa Massimino** and **Chuck Cosson,** and asks them what the opportunities and challenges are for working with businesses in this field.

Elisa Massimino explains that they have a history with working with businesses, including working with the apparel industry to enact labor standards. She gives a lot of credit to Microsoft, Google, and Yahoo who are working together in the Global Network Initiative, to set standards for when they will disclose user information to governments. A perfect storm where some kind of crisis occurs that threatens lawsuits or damages a company's reputation is typically necessary to initiate such a partnership. There's a question of trade-offs in working with companies because solutions are never absolute, and change will be incremental. Freedom in the virtual space is a top issue for human rights activists, though, and it's necessary to engage with the corporate players in the field.

Chuck Cosson explains that there are many smaller companies who build on Microsoft platforms and NGOs who use their tools or donated technologies, so they have a history of working to further human rights/NGOs' work. In the last four years, the importance of the human right to free expression and privacy and the use of digital media has come to their attention, particularly with operating in China. By working with NGOs and human rights advocates, they get information about what people are doing and how their technology is used or misused, expertise in the field of human rights, and guidance for how the company should respond. In turn, they get an opportunity to influence how their advocacy and ensure that it is informed. Corporations do have different missions since obligations to shareholders come first, but these are broader and deeper than the next quarter's profits. Elisa Massimino agrees that a world in which rights are respected is a better, more stable, more profitable world for the information technology sector, so there is a long term convergence of interest.

Q: Are excitement and emphasis on digital technology distracting from important issues? In human rights, so much important work is done on a local level, and by local communities.
A: Andrew Puddhephatt comments we shouldn't create such a stark divide between local/analog and international/digital – even for people living in villages, the ability to network beyond your immediate surroundings is a key characteristic of affluence (e.g., the spread of phones in Africa).

Q: What about about encryption technologies so that users can themselves ensure their privacy?
A" Chuck Cosson comments that the policy debate on encryption has in many respects played itself out, because governments realized that without encryption the world couldn't operate (e-commerce, finance, etc). Also, Microsoft is looking at ways that people can use things other than a username/password combination since this can be vulnerable to hacking or trickery.

Comments from participants:

- The important thing about digital technologies is that our activists have more choices, so the question is what they should fund to help their grantees be more strategic in using them.
- Everyone should consider access and security issues for technology for people with disabilities.
- Don't get carried away with how fantastic technology is – need to think about content, too. How do you tell what level of market saturation is a critical mass to catalyze change?
- Young activists in Egypt have made great use of technology – how do you compare their success with groups like Hezbollah and the Muslim Brotherhood?
- When funding technology efforts, always ask what campaign that technology will be used for.
- What they can we do as funders to protect advisors and grantees, and how do we balance transparency with protection?

Panel comments:

- Brett Solomon agrees that there is often too much cool technology and not enough user-generated means taking advantage of it. To catalyze change, it's not about the quantity of saturation of technology but who those users are, so they focus on "bespoke" technologies to give the right technology to the most important people (start from demand, not supply).
- Elisa Massimino adds that the traditional process of figuring out your objective and obstacles to overcome still holds, but the new challenge is to be familiar enough with new technology since it often will have a direct bearing on your ability to succeed. Sometimes it's about numbers (e.g., mobile phone use to organize meetings/protests), but more often it's about *who* has access.
- Andrew Puddhephatt says that he is thinking of asking some grantees to send reports of who's accessing their web resources, which gives some indication of impact and demand (you can find out where and who the hits are coming from through IP addresses).
- Thomas Hughes adds that we can learn from the advertising world in terms of how they track views of web media and their impact. There's a difference between putting out tools (which can be used by anyone) and putting out content.

Q: What should funders do about companies who cooperate with governments that ask them to divulge user information?
A: Elisa Massimino responds that this is a hugely important question, and it's one of the major projects of the Global Network Initiative. Environmental and labor issues have historically been easier to

advocate than human rights, but the same dynamic that exists with US companies and anti-corruption standards could be pushed to digital issues. Some companies publicly post all requests to divulge private information, which helps them to understand the parameters of the problem.

Q: Is there a distinction between the pressures that applications companies like Google and Yahoo face, and those that Microsoft faces?
A: Chuck Cosson responds that creating guidelines for responding to demands is a major reason for the Global Network Initiative. And in many cases governments ask for information to defend human rights (eg, investigating a kidnapping). Standards are needed that can be applied worldwide to do the right thing and avoid unintended consequences. Risk assessments such as consulting Freedom House rankings should be done before setting up a data storage site in a country (which gives that government sovereign rights over all of that data). It's also important to ask for demands in writing and for justifications. Generally, GNI is aimed at asking governments to follow a process that lives up to treaty commitments and rule of law. Companies should also be more transparent about what policies they have on data security. Hardware companies are in a different position than software companies since software companies can control over how they respond to a demand, but if you sell a hardware product, you can't control how it's used. But for cases like China demanding built-in filtering systems, collaboration among companies is key.

Andrew Puddhephatt closed the session by emphasizing the importance of collaboration, and of digital literacy in the human rights community.