INTERNATIONAL HUMAN RIGHTS FUNDERS GROUP

SEMI-ANNUAL CONFERENCE
SAN FRANCISCO
JANUARY 24-25, 2012

Hacked, Hassled, Silenced: Grantmakers Role in Navigating Internet Security

Tuesday January 24, 2012
3:15 pm – 4:45 pm

***Session Organizer*:**

- Kathleen Reen, Vice President for Asia, Environment, and New Media, Internews

***Panelists*:**

- Bob Boorstin, Director of Public Policy, Google
- Kathleen Reen, Vice President for Asia, Environment, and New Media, Internews

Sponsors:

- Internews

Introduction:
This session discussed the role of security in human rights as it relates to technology and its relationship with media, policy and access to information. Internews, founded 30 years ago and based in CA, is an organization devoted to the idea of creating quality information among media and human rights organizations. By the time they got to the Asia region, found a different problem and challenges.

Some key issues that Internews has focused on are:

- The availability of software access for NGOs to move securely as they go about their work;
- Education and outreach: articulation of these problems is difficult and very few people understand how technologies work (internet, phone, etc.);
- Discrepancy in mobile technology accessibility/availability: In ¾ of countries, mobile penetration had more than doubled. During the Arab Spring, they saw that use of mobiles made a 39% jump in Egypt. Tunisia had only 77% before the revolution and jumped to 106%. Meanwhile, mobile use in Burma is 1.24% - which means that less than 1 million people have regular access to internet or mobile phone.

Bob Boorstin, Google:
Google makes grants to groups working in the area of human rights/online free expression. They are interested in keeping the internet safe for democracy and dissent. Google makes grants to Internews and others on the frontlines for access to information. Google provides a platform for people to express themselves, but is not in the business for regime change.

Kathleen:
Some issues to watch for in this realm:

- Human rights activists using mobiles, internet cafes etc. are putting themselves and people in their networks at risk of torture and death. Government-owned telephone companies can easily track them.

- This is a difficult area to understand because of how fast-changing technology is.
- Human rights advocates are using same tools as governments, which are using smart people to counter the other side.
- Technology users do not have an understanding of the technology they are using or how to stay safe using that technology. This is found more amongst traditional human rights groups (who have been on the front lines for years and have been successful in running campaigns, etc.)
- Mobile technology: if funders are not funding people doing mobile work then they are "nowhere" – this is the future. People are not going to be accessing information through laptops and Ipads, but through mobiles. Not even smart phones but level 2 or 3 phones (SMS and basic functionality).

Lessons learned by Internews:

- Internews had security embedded in all of their work, but it was challenging to get their head around the problem and harness solutions.
- A nonprofit investing in R&D solutions for internet security has been integral. A percentage of all of the projects they fund is committed to this issue (keeping partners, people safe). Surveillance, censorship, interference is a huge risk.
- Internews has been asking partners to invest in the equivalent of IT specialists and CTOs (Chief Technology Officers).
- Strategic partnerships: problem is so ubiquitous that it is essentially to partner with people who are doing this work/committed to this issue. This is an under-funded area and it is moving fast.

Experiences of Funders Participating in the Session:

James Logan-Oak Foundation: Oak has been funding this issue for years and they see that some organizations focus on pieces of this issue, but they rarely know about one another. In terms of training methodologies: human rights organizations are resistant to new approaches. They have trainers parachute in for trainings and leave after a few days without integrating the security training into the work of the partner organizations. One idea is to do more context/grantee specific trainings where the trainer looks at the specific needs of the organizations, designs solutions, implements it, and then follows-up as necessary. In addition, trainings reach a small number of grantees, but this issue affects a much broader range of protesters or others who have never engaged in traditional human rights work. They are highly vulnerable if they are using mobiles, etc. How do we deliver training and capacity building to this group (of non-grantee/non-traditional human rights activists)?

Comment from Bob: When there are a limited amount of funds, there is no choice but to pick groups that are doing the best job and willing to share their learning. It is important to fund projects that operate on "open share" and platforms that can be built on and not projects that are closed. The danger with the open share platforms is that governments can send an engineer to build on it and add Spyware, which will infect the computer.

In other cases, they have encouraged groups to join/merge for better utilization of resources. Fragmentation in the tech world is inevitable because the field moves so quickly. Individuals often think they have latest/greatest thing.

In terms of reaching a limited number of people with training: encourage people to put together online tools that are part of trainings/workshops that anybody can download/look at to understand something more about their area. This is a way to make progress.

Comment from Kathleen: Funders should make space for the chance that some investments may fail. This gives partners some latitude to explore, which fosters creativity. Govt. donors have shown tremendous interest in this area.

The power of convening this group is still in its early stages. Govt. donors are funding this area. Private sector is absent from this sector. In the Arab Spring, they saw 10-20 organizations pulling resources together and sharing information. There was a huge back-end to Tahrir Square – people all over the world worked together in real time to keep internet open and up and train people in real time. Traditional training model is expensive/face-to-face is hard to afford. Therefore investing in online training tools in local languages and context is a great alternative. Real time situation changes so fast that there isn't time for traditional training. The problem is that people who are trying to teach security do not know security themselves. We need to build a team of security experts in human rights organizations (ideal person is IT staff at human rights orgs/foundations).

Question: Who is getting most attacked by security related incidents? What resources would they recommend for what organizations can do to protect themselves?

Answer from Bob: Most attacks are on active NGOs in politically-difficult countries. Mostly Diaspora groups in Iran, China, or Syria are undergoing hacks and attempts to put Malware on their computers (which destroys the computer or allows someone to read files). There are also attacks on groups/people taking down websites (ex: Iran). Websites of corporation with high-tech or dual-use technology are also being attacked. Corporations are being attacked on huge and ongoing basis by governments trying to seek technology transfer without paying for them. (Ex: China attacked Google and 32 other multinational corporations). Transparency is important for people under attack – they should speak out to educate others in the field so they can protect themselves.

Kathleen: Internews has seen an increase in partners that are asking for help. There is a website in Syria ("Syria for all") which has been attacked twice. Malaysia News Service has been attacked 3 times. There is 2nd and 3rd generation of technology being developed by governments or criminal networks that vastly overpass their ability to deal with these challenges (not enough resources and they must change the paradigm of sharing information to affectively combat it).

Organizations are now addressing security holes in their software. A great tool can be created which can revolutionize how organizations report on conflict. However, it will also have vulnerabilities because it needs to be maintained continuously. This is another challenge: this work never ends/goes away. They are also noticing that national organizations are starting to address this issue.

Resources recommended: MobileActive, Tactical Tech are two resources. The latest collection of useful resources can be found at "Open Initiative" (a consortium of groups at universities), and also at Global Voices.

Question from Romdhani: The revolution in Tunisia has been seen as an "Internet Revolution." The Internet has taken an important role as a means/tool to the revolution, but was not the trigger. Having a monopoly on information was the most important thing to the dictator. Communication has helped organize the revolution. After the revolution, people realized that individuals working for the government are not the police but highly skilled engineers. People are still trying to control competitive ideologies by manipulating information. How should we address this?

Answer from Bob: Agrees that the internet is a tool and not a trigger of the revolution. People in this field have gotten carried away with the significance of the tool. Also agrees about breaking the

information monopoly. It is a slippery slope. Many websites go to moderation where they actually have people looking at whether comments are constructive or false/destructive. The problem with editing is the line: when do you go from moderating a site to clamping down on the individual right to expression? No one has been able to answer this question. Now anyone can be a journalist on the internet and the same ethics do not apply. Google does try to moderate hate speech. It is a difficult line to draw however. Societies like Tunisia are coming to grips with multi-party civil societies will have to figure out how these lines are drawn.

Comment from Kathleen: Many countries have organizations that focus on national policy around the technology regulatory environment and addressing this question. Compare other countries that are similar (ex: Indonesia). Give it time to evolve.

Question from Conrad: Meetings have been held in Washington DC where there were lots of arguments around privacy and digital encryption. One of the arguments was that the private sector would provide digital encryption. People who were building it wanted point and click privacy so that they are able to send "packaged" emails. What happened to hard encryption being built into the system?

Answer from Bob: This is an ongoing debate: how can they provide the best services and protect people. Google does it by making searches on "https" which means it is encrypted. At the same time, in the tech industry there is a growing movement towards compiling data in a better way than the competition and delivering what the consumer wants. Google has insisted that a user of Google be able to remove data at any point he/she is dissatisfied with information: "Data Liberation Front" "Cage Free Data." Google also has a dashboard that allows you to save what you do/don't want it to remember. But he does not think this will ever be solved because when you give people the option to get out, they blink right by it. Ex: people accept privacy agreement when viewing a website. Even the most educated people are not objecting to privacy policies being put before them, so the average person will not stop to read/opt out. Google has taken 7 different privacy policies and boiled them down to 1. Corporations do owe users transparency about data, ability to take data out, and control what company is getting from you. There will not be a perfect answer in this area though. It is a problem that the Internet poses. And there is a problem offline too (health insurance companies know more than what Google knows).

Follow-up question from Conrad: Why doesn't Gmail allow PGP? ("pretty good privacy" – encryption program – it cannot be intercepted without extreme computing power).

Answer from Bob: Most companies would say that the user-experience would be severely degraded. But he is not a privacy or technology expert but happy to take this question to the engineer at Google.

Comment from Kathleen: Welcomes and wants to see more interdisciplinary work in the area of human rights organizations communicating with companies about their needs. The current dialogue is weak.

Question: US government agencies have devoted aid to online security – how will that play out and how does that funding interact with Internews' projects?

Answer from Kathleen: There has not been much redirection. US funds come out of earmark introduced in 2007 where $30 million were made available for internet freedom. Subsequently, they have asked to take a closer look at the security question. This has been an open conversation. The Secretary of State made the first speech about this in 2010. USAID made a commitment in 2011 to provide specific funding with focus on this. It is still fairly new. Policy makers and administrators in USAID and State department are deeply committed to it. The community of people that is concerned has grown. Bridges have been built to European AID agencies also. Private foundations made commitments earlier. Government

donors have taken longer to get there. The US government is not the first government to fund this. Europeans were first as part of a human rights defenders program. They grew organically as partners began to invest in this area.

Question: The future will be basic mobile technology, but with regard to government surveillance, what are your views on interception laws in the US and abroad?

Answer from Bob: Governments will continue to try to monitor more. Companies face a problem that they are expected to be intermediary that protects users. However in these cases, the government asks them to hand over information. Google tries not to store information in certain countries where they know it will be vulnerable to seizure. They have joined the Global Network Initiative where companies are joining one another in arguing against governments.

Comment from Kathleen: It is a fairly even playing field right now. In Australia, the debate has been focused on child protection. Child protection organizations have been powerful and efficient in bringing their issues to the table and prioritizing. But balancing them out and maintaining openness is a challenge. This will be an expanded problem in any country and part of the security assessment.

Comment from Bob: Laws are being written in developing countries that say that if you offer products/services than you must build a data center in our country. Because of privacy and other concerns, Google will not do this.

Question: Helping grantees keep their information secure, but also weighing public policy concerns – what should donors focus on?

Answer from Kathleen: With the high penetration of technology now the big shift will be from basic phones to data phones. Real trends are in regulation, freedom of expression, privacy and access to information. A new trend is US domestic organization partnering with international NGOs because they are in the same fight. Data retention is a challenging area. There are not enough qualified lawyers and experts to tackle this issue. There is also a shortage of academics, experts, and knowledge by lawmakers on these issues. In 1990s after fall of Soviet Union, many donors funded tech as part of anti corruption work, but then there was a fall off and this area became under-funded. Donors get bored with policy change and it takes a long time. Create at least interdisciplinary dialogues for these conversations to take place.

Comment from Bob: A good source for donors is the OECD principles which define the coming framework for what the internet should look like

Question: Security from the human rights defender/funder perspective, how do we link awareness about this issue with behavior change?

Answer from Kathleen: There are a series of online campaigns in 12 languages targeted at the biggest offenders of Internet surveillance and interference. They worked with local advertising companies to create ads that reached 1 billion people. Defenders and funders can use tech tools out there to create metrics in this area.