

# **TWITTER AGAINST TYRANTS: NEW MEDIA IN AUTHORITARIAN REGIMES**



**OCTOBER 22, 2009**

**Briefing of the  
Commission on Security and Cooperation in Europe**

---

**Washington: 2012**

**Commission on Security and Cooperation in Europe**  
**234 Ford House Office Building**  
**Washington, DC 20515**  
**202-225-1901**  
**csce@mail.house.gov**  
**http://www.csce.gov**

**Legislative Branch Commissioners**

**HOUSE**

ALCEE L. HASTINGS, FLORIDA,  
*Co-Chairman*  
EDWARD J. MARKEY, MASSACHUSETTS  
LOUISE McINTOSH SLAUGHTER,  
NEW YORK  
MIKE McINTYRE, NORTH CAROLINA  
G.K. BUTTERFIELD, NORTH CAROLINA  
CHRISTOPHER H. SMITH, NEW JERSEY  
ROBERT B. ADERHOLT, ALABAMA  
JOSEPH R. PITTS, PENNSYLVANIA  
DARRELL E. ISSA, CALIFORNIA

**SENATE**

BENJAMIN L. CARDIN, MARYLAND,  
*Chairman*  
CHRISTOPHER J. DODD, CONNECTICUT  
SHELDON WHITEHOUSE, RHODE ISLAND  
TOM UDALL, NEW MEXICO  
JEANNE SHAHEEN, NEW HAMPSHIRE  
SAM BROWNBACK, KANSAS  
SAXBY CHAMBLISS, GEORGIA  
RICHARD BURR, NORTH CAROLINA  
ROBERT F. WICKER, MISSISSIPPI

**Executive Branch Commissioners**

MICHAEL H. POSNER, DEPARTMENT OF STATE  
MICHAEL C. CAMUÑEZ, DEPARTMENT OF COMMERCE  
ALEXANDER VERSHBOW, DEPARTMENT OF DEFENSE

## ABOUT THE ORGANIZATION FOR SECURITY AND COOPERATION IN EUROPE

The Helsinki process, formally titled the Conference on Security and Cooperation in Europe, traces its origin to the signing of the Helsinki Final Act in Finland on August 1, 1975, by the leaders of 33 European countries, the United States and Canada. As of January 1, 1995, the Helsinki process was renamed the Organization for Security and Cooperation in Europe (OSCE). The membership of the OSCE has expanded to 56 participating States, reflecting the breakup of the Soviet Union, Czechoslovakia, and Yugoslavia.

The OSCE Secretariat is in Vienna, Austria, where weekly meetings of the participating States' permanent representatives are held. In addition, specialized seminars and meetings are convened in various locations. Periodic consultations are held among Senior Officials, Ministers and Heads of State or Government.

Although the OSCE continues to engage in standard setting in the fields of military security, economic and environmental cooperation, and human rights and humanitarian concerns, the Organization is primarily focused on initiatives designed to prevent, manage and resolve conflict within and among the participating States. The Organization deploys numerous missions and field activities located in Southeastern and Eastern Europe, the Caucasus, and Central Asia. The website of the OSCE is: <[www.osce.org](http://www.osce.org)>.

## ABOUT THE COMMISSION ON SECURITY AND COOPERATION IN EUROPE

The Commission on Security and Cooperation in Europe, also known as the Helsinki Commission, is a U.S. Government agency created in 1976 to monitor and encourage compliance by the participating States with their OSCE commitments, with a particular emphasis on human rights.

The Commission consists of nine members from the United States Senate, nine members from the House of Representatives, and one member each from the Departments of State, Defense and Commerce. The positions of Chair and Co-Chair rotate between the Senate and House every two years, when a new Congress convenes. A professional staff assists the Commissioners in their work.

In fulfilling its mandate, the Commission gathers and disseminates relevant information to the U.S. Congress and the public by convening hearings, issuing reports that reflect the views of Members of the Commission and/or its staff, and providing details about the activities of the Helsinki process and developments in OSCE participating States.

The Commission also contributes to the formulation and execution of U.S. policy regarding the OSCE, including through Member and staff participation on U.S. Delegations to OSCE meetings. Members of the Commission have regular contact with parliamentarians, government officials, representatives of non-governmental organizations, and private individuals from participating States. The website of the Commission is: <[www.csce.gov](http://www.csce.gov)>.

# TWITTER AGAINST TYRANTS: NEW MEDIA IN AUTHORITARIAN REGIMES

OCTOBER 22, 2009

## COMMISSIONERS

	Page
Hon. Sam Brownback, Ranking Member, Commission on Security and Cooperation in Europe .....	2
Hon. Robert B. Aderholt, Commissioner, Commission on Security and Cooperation in Europe .....	7

## PARTICIPANTS

Kyle Parker, Policy Advisor, Commission on Security and Cooperation in Europe .....	1
Daniel Calingaert, Deputy Director of Programs, Freedom House .....	3
Nathan Freitas, Adjunct Professor, NYU Interactive Telecom Program .....	5
Evgeny Morozov, Yahoo! Fellow, Georgetown University; Contributing Editor, Foreign Policy .....	8
Chris Spence, Chief Technology Officer, National Democratic Institute for International Affairs .....	10
Shiyu Zhou, Deputy Director, Global Internet Freedom Consortium .....	12

## APPENDICES

Prepared statement of Nathan Freitas .....	30
Prepared statement of Evgeny Morozov .....	35
Prepared statement of Shiyu Zhou .....	39
Material submitted for the record by:	
Oleg Brega, filmmaker, journalist, civil society activist from the Republic of Moldova .....	42
Mark Belinsky and Emily Jacobi, Co-Directors, Digital Democracy .....	44
Mary Joyce, Andreas Jungherr, and Daniel Schultz, Working Group on Sanction Reform for the Digital Age [DigiActive.org] .....	48
Patrick Meier, Director of Crisis Mapping and Partnerships, Ushahidi .....	50
Merici Vinton .....	53

# **TWITTER AGAINST TYRANTS: NEW MEDIA IN AUTHORITARIAN REGIMES**

---

**OCTOBER 22, 2009**

## **Commission on Security and Cooperation in Europe Washington, DC**

The briefing was held at 2 p.m. in room 1539, Longworth House Office Building, Washington, DC, Kyle Parker, Policy Advisor, Commission on Security and Cooperation in Europe, moderating.

*Commissioners present:* Hon. Sam Brownback, Ranking Member, Commission on Security and Cooperation in Europe; and Hon. Robert B. Aderholt, Commissioner, Commission on Security and Cooperation in Europe.

*Panelists present:* Kyle Parker, Policy Advisor, Commission on Security and Cooperation in Europe; Evgeny Morozov, Yahoo! Fellow, Georgetown University; Contributing Editor, Foreign Policy; Chris Spence, Chief Technology Officer, National Democratic Institute for International Affairs; Shiyu Zhou, Deputy Director, Global Internet Freedom Consortium; Daniel Calingaert, Deputy Director of Programs, Freedom House; and Nathan Freitas, Adjunct Professor, NYU Interactive Telecom Program.

Mr. PARKER. Folks, we're going to go ahead and start. Thank you for coming to today's Helsinki Commission briefing on new media in authoritarian regimes. I apologize for starting late—we are expecting the possible presence of some of our Commissioners, so if they do come, we'll turn the floor over to them. This is a briefing, it's being transcribed and I think televised on the HouseNet. Unlike an official hearing, we will be taking questions from the audience, so as you listen to the presentations please be thinking about good questions so we can have a good, lively, informative, and somewhat informal conversation today, and that also goes for the panelists. We can certainly talk amongst the panel as well.

I'm not going to spend too much time introducing the topic. The Helsinki Commission is an organization going back to 1976. We monitor the implementation of the Helsinki Accords, the Helsinki Final Act across 56 participating States. The United States is one, all of Central Asia, Europe and Canada as well. And one of the fundamental freedoms enshrined in the act is of course the freedom of media, and of course it's often through that, either freedom of media or freedom of speech, freedom to communicate, that we learn of other infringements or other issues, be it religious freedom or freedom of assembly. Obviously, if you don't have a telephone or a newspaper or an e-mail, it's hard to hear about those things.

Another thing we do quite often is election observation; in this past year, two very prominent cases, Moldova and Iran, where technology such as Twitter played quite a major role. And I'm happy to have Senator Brownback. Senator Brownback, ladies and gentleman. Take a seat.

Mr. BROWNBACK. Sorry to come in late, I apologize about that.

Mr. PARKER. No problem, no problem. [Inaudible, off mic.]

Mr. BROWNBACK. If you don't mind letting me make a quick statement. I apologize to people for arriving late on a very important topic, and my apologies for doing it. I have a brief opening statement I'd like to make and then hear the panel presentation. I'm delighted to see this hearing taking place. I think we saw this demonstrated in real-life form in the Iranian elections and the follow-up afterwards, of how Twitter turned against the tyrants in Tehran.

Chairman, I want to thank the committee and the Commission for holding this very important and timely hearing on the crucial role that new media plays and will continue to play in closed authoritarian societies. As we approach the 20th anniversary of the breaking of the Berlin Wall, we must gather our strength and commit ourselves to finding ways to tear down the new walls of the 21st century, the cyber-walls, the electronic censorship technology used by tyrants to repress the free expression of millions and millions around the world. I look forward to learning from these distinguished panelists how we can move forward on this issue.

I'd first say a quick word about the freedom of information, and specifically Internet freedom. If information is the adrenaline of democracy, then our Internet-driven society is on high endorphins. Individual citizens have never before had so much access to real-time political, economic and social information affecting their lives, and generally this has led to increased accountability and better outcomes. Recently, we've seen the other side of the information spectrum. In Iran, this past summer, the real battle took place and is still taking place on blogs, Facebook and Twitter as Iranians struggle to tell their story while the regime desperately tries to block access to the Internet. The same was true for the Burmese opposition in 2007, where the junta struggled to contain the fallout from its bloody crackdown. Before that, text messaging played a crucial role in the Orange Revolution in Ukraine.

One thing is clear: While physical brutality will always be the tool of oppressors, 21st century authoritarianism has already been defined by the lengths to which autocrats will go to limit online access to information. The Iranian dictatorship, the Chinese Communist Party, the Burmese junta, the Castro regime and other regimes worldwide all derive a large share of its power through media suppression and rigorous Internet censorship.

Before we discuss how to tackle this problem, I think we must understand its cause. Why do regimes monitor, limit or even block the use of the Internet? Surely allowing open use of the Internet, a modest investment, would make life for residents of these societies more bearable and more efficient. And the answer, clearly, on the regime's parts is control and survival. Free and open access of the Internet would allow unfettered criticism of regimes that sustain themselves only by forcibly perpetuating the appearance of perfection. These dictators not only shield their population from their own brutality but also block information about the basic freedoms enjoyed by millions worldwide.

Leaders of these oppressive regimes disdain criticism and challenge because it pushes back against this fiction of success they pedal to the masses. As the fiction crumbles, their

grab on power dissolves. Like with the Polish Solidarity Movement, the defiance of the people eventually cracked the defiance of the government. This is why we must focus our efforts on promoting the freedom of information, specifically Internet freedom. As individual information exchanges become effortless through wireless communications, authoritarian regimes must devote ever-more resources to maintain their electronic wall. If information is power, then it is time to help bring the power to the people.

We must ensure that all closed-society residents have free and open access to the Internet. This is the surest and most cost-effective way to jumpstart liberty. Indeed, the more the oppressed see and understand the real nature of their regime and the more they share with the outside world, the more power they will have to determine their own future. This is a key effort on our part to open up the Internet to regimes and to the people in these regimes that suppress their action and their access to it.

So it's my hope that hearings like this one today, will help us in getting funding for groups that provide access to Internet, to Twitter, to Facebook, to other social media, that we can provide that and help these, in many cases, very difficult operations that people are putting together on private dollars to open up the Internet to people that don't have access to it themselves. So I hope that we can do that. I want to thank the panel very much for allowing me to come in a little bit late and put forward that statement, and I look forward to hearing some of the comments from other individuals here.

Mr. PARKER. Thank you, Senator. We can proceed with the panel, starting with Daniel Calingaert, Deputy Director of Programs at Freedom House, and I might add that the—more extensive biographies should be on the table outside and will be posted on our Web site, but we'll just—given the fact that we have five panelists, we'll go ahead and start with the discussion. So Daniel, please.

Mr. CALINGAERT. Yes, thank you. Thank you, Kyle, and many thanks to the Commission for inviting me, and Senator Brownback, we very much appreciate your interest and leadership on this issue. New media has created significant opportunities for advancing freedom in countries ruled by authoritarian regimes. It has expanded the space for free expression and facilitated civic activism. But authoritarian regimes have pushed back. They have restricted Internet freedom in a variety of ways, and they are likely to further limit the space for free expression and civic activism on the Internet unless the U.S. Government works proactively and vigorously to keep that space open.

The impact of digital media on authoritarian regimes was evident in Iran following the rigged Presidential election of June 12th. Digital media made important contributions to the Green movement of post-election protests. The movement's leader, Mir Hossein Mousavi, communicates to Iranians primarily through his blog and Facebook. Protests are announced and organized largely via the Internet, and images of police crackdowns and of defiance by protestors often are transmitted across Iran and to the outside world through Facebook and Twitter with the help of anti-censorship technology.

The Green movement was sparked by public anger over the blatant electoral fraud committed by supporters of President Mahmoud Ahmadinejad, but it is kept alive in large part by the use of new media. Citizens in the former Soviet Union have used new media to assert their rights and to challenge abuses of power. In Russia, for example, the Internet was the primary means for drawing attention to fraud in this month's local elections. When observers in the Moscow district of Zyablikovo found a group of individuals hired to vote for United Russia multiple times, they used Twitter and Livejournal blogs to spread the news immediately and to publish photos of the violators.

A member of that district's electoral commission, Andre Klukyn gave an online interview to describe in detail the plan behind this fraud. The interview was widely viewed on Russian YouTube and covered by several traditional media outlets. Another group of observers published video footage of a polling-station chairman in the city of Azov as he tried to mix fraudulent ballots which had already been filled in for United Russia with legitimate ballots. This video became a hit in the Russian blogosphere and prompted a criminal investigation of the polling-station chairman. Digital media spread the news of voter fraud in Russia's local elections and contributed to a real-world response. The news triggered a public demonstration on October 12th in Moscow's Pushkin Square and prompted all three opposition parties to walk out of Parliament in protest.

In Belarus, traditional media is highly restricted. In the Freedom House ratings of freedom in the press, Belarus is near the bottom; it's ranked 188th out of 195 countries. But the Internet actually provides extensive space for free expression and activism. Most Internet users in Belarus turn to non-state sources for news. In fact, of the top 20 news and information Web sites, only 3 are state-run sites, 12 are independent or pro-opposition and the rest focus on sports or other non-political subjects.

I can also point to another example of online activism in Kazakhstan, where there was a new law passed in July to restrict the Internet, and while that law was being considered, a local free-speech group, Adil Soz, organized an online campaign that used blogs and Facebook and Twitter to mobilize opposition to the bill. And there was also, obviously, international criticism of the bill and criticism in other places in Kazakhstan. The bill eventually passed, but one of the key provisions, which would have given prosecutors the authority to suspend media outlets without a court order, that provision was removed from the law. So I think the online campaign had some effect.

While new media plays an important role in expanding free expression and facilitating citizen engagement, it does not drive political change. New media alone cannot undermine authoritarian regimes. Authoritarian regimes in the former Soviet republics and elsewhere continue to repress their citizens, and this repression extends to digital media. In Russia, for example, Internet freedom has declined significantly in recent years, as bloggers have become subject to hacker attacks, legal prosecution and physical violence. Although there is no technical filtering in Russia, officials often make phone calls to pressure web hosts or Internet service providers to remove unwanted content. The director of a leading hosting company, Master Host, admitted that his company gets about 100 requests a day to remove content from inconvenient—so-called “inconvenient” Web sites.

In Belarus, authorities conduct surveillance on Internet users, and they require cyber cafes to register each user's browsing history. Kazakhstan's Government, as mentioned before, introduced a law in July to regulate, but really to restrict, the Internet, and this law makes all forms of Internet content, whether Web sites, blogs, chat rooms, subject to the same restrictions that are in place for traditional media.

The restrictions on the Internet are likely to increase unless citizens in Russia, Kazakhstan and elsewhere struggle to keep the Internet open, and this struggle requires U.S. support. Authoritarian regimes use a variety of methods to limit online freedom of expression. The United States therefore has to respond in multiple ways. This response should consist of, first, preventing the use of U.S. technology in violations of Internet user's rights, second, building effective coalitions among democratic governments in defense of Internet freedom. Third, investing in technology to circumvent censorship and strengthen user privacy and fourth, but certainly not least, supporting indigenous efforts

in the country's where the Internet is restricted, supporting their efforts to expand the space for free expression online.

The Internet is a medium for communication. Its impact on authoritarian regimes ultimately depends less on the medium itself and more on the messages it conveys and on the messengers who use it to drive progress toward democracy. Therefore, we should not only invest in anti-censorship technology, but also support the creation and distribution of pro-democracy content and back the courageous and creative activists in repressive environments who are struggling to bring about political change. Thank you.

Mr. PARKER. Thank you, Daniel. We will now move onto Nathan Frietas, who is adjunct professor at NYU, interactive telecom program and leading protest software developer. Nathan?

Mr. FRIETAS. I'm going to try to walk the walk and use my mobile phone. So I greatly appreciate the opportunity to participate in this hearing, Senator Brownback, the Chairman of the Commission.

For me, I come as a representative of the countless technology and new media advocates who believe that the most amazing and groundbreaking innovations of our generation should be used for more than the acquisition of wealth or distraction or entertainment, but should be used to really do good in the world.

I'm also a long-time member and former board chair of the international group, Students for a Free Tibet—working with Lhadon Tetong and Tenzin Dorje. What I'll share with you today is some of my experiences as an activist-practitioner, on the ground, employing these technologies both in the United States and abroad.

A bit of history on Twitter—the roots of this new media technology wave and specifically, Twitter, began in 2004 with an open source Web service called TXTmob. TXTmob was developed by MIT's Institute for Applied Autonomy and used at the 2004 DNC and RNC conventions, specifically, RNC in New York. I was part of a team that utilized this to broadcast tens of thousands of messages to thousands of people on the street to let them know what was going on, what the breaking news was.

Later this same technology was used in the Orange Revolution in the Ukraine to create flash mobs and coordinate sit-ins. In 2005, two of my colleagues who worked with TXTmob were employed by the company that became Twitter. And they began showing this technology around the office to see the power of short-message broadcasting. So Twitter was born out of an activist movement, so it's no surprise that it's come full circle and is being used that way again.

My specific area of work is focused on Asia, specifically China, Tibet and India. I've been employed in Silicon Valley and Silicon Alley. I developed patented technology and was a student at the University of California, where I worked on DARPA and NSF-funded research. So I'm a product of the both government-funded and private-funded efforts to develop new technologies. Now, I'm fortunate to be teaching at NYU's Interactive Telecommunications Program, the course titled: "Social Activism using Mobile Technology."

This is a one of the first of its time courses and I believe more education opportunities like this should be given to students to understand the alternative opportunities they have coming out of school. My path might seem novel, but it comes from a long history of geeks, nerds, and engineers who want to apply their skills to helping their country and their community. During the Second World War and the cold war, inventors, mathemati-

cians used the first digital computers to play a critical role in the Allies' efforts to stay in front of the Axis.

During the Civil Rights movement the use of telephones, telegraphs, and traditional social networks in churches and universities created a foundation to mobilize supporters throughout the South. And in recent years, hackers, nerds and geeks like myself have gravitated toward the social justice, environmental and human rights movements.

So the idea of two guys in a garage in Silicon Valley has translated into teams of activists around the world using Skype, Facebook, and Twitter to innovate and develop new systems to use the same grassroots organizing and non-violence techniques that have come from Gandhi, but in a new era.

We already mentioned Burma and I believe it will come up again. The fascinating thing about what happened in Burma in 2007 was the emergence of the video journalist. Someone with a very cheap digital camera broadcasting their message using the Internet: instant messaging, FTP file transfer—and ending up on the BBC. So the official view—and this is, sort of, the early days of YouTube and they didn't use that. The idea that they could do that to cover their movement and even though the Saffron Revolution wasn't successful, the impact they left in the world of activism about the possibility was very successful.

A similar model is being used in Iraq through a video channel called Alive in Baghdad which, what that does, is represent an alternative option for Iraqis to express themselves and their situation rather than turn to violence. The power of the moving image is unavoidable. And with the low cost of distributing videos online, the ability to easily stream it live from mobile phones or satellite data networks means that its reach and impact has come to rival broadcast television.

In many cases, authoritarian states' powers prove too formidable for new media technology. We saw this with Tibet in the uprisings last March. The only view that the world had of the uprising was from the Chinese state media. Internet was cutoff, phone was cutoff, and reporters from around the world were blocked from accessing an area the size of Texas. So in that case, the type of infrastructure that China has been able to put in place is overwhelming.

And working with American companies such that they do not provide the technology to censor, filter, surveil, and block is an important outcome that I would like to see from these discussions. The other way technology has been used for activism is when outsiders move into a country—activists, human rights workers, fair election advocates—to use technology in a place that allows them to be more efficient.

So election monitoring, or for instance, last year during the Beijing Olympics when all protest was not allowed, over 70 activists traveled there with camera-phones, small portable computers, high-definition video cameras—and were able to protest and document their work—more on that in my statement in this paper.

Finally, last year during the Presidential election, I worked on a project called Twitter Vote Report. This was a nationwide Web 2.0-style project for election monitoring that allowed people using SMS, iPhones, or standard telephone in English or Spanish to report in problems that they had at the polling place. We had a real-time Google Map, a real-time alerting system for any delays or ballot issues. That was a very successful project that's being replicated in Afghanistan, recently, and elsewhere.

So as you can tell, I'm a very enthusiastic and active participant in the use of new media tools for social good. However, the use of these tools brings serious risk to the user, their friends, family, and broader movement. As a friend of mine said, you cannot Twitter your way out bludgeoning by security goons. Mobile phones are unique identifiers that track their user. Laptop computers are full of incriminating documents. Digital viruses deliver powerful espionage tools such as GhostNet. One slip and your entire e-mail box and social network can be revealed.

So we need to spend more time focusing on protecting activists, protecting these generations that take 20 years to rebuild if they're decimated. And while the free world is enamored of these tools and we're here with this hearing, our own Federal, State, and local law enforcement are often quite fearful of their use at home. So just recently, Elliot Madison, a 41-year-old social worker, was arrested in Pittsburgh and charged with hindering apprehension for prosecution, criminal use of a communication facility, and possession of instruments of crime.

He was found with a computer and was using Twitter. This is a contradiction that we must address and come to term with. We do want to protect our homeland from violent terrorists and we do want to apply these tools fairly. But we need to make sure that we understand their impact on the domestic front.

So there are constructive steps that we can take. We continue to support the freedom of media and extend that to the conduits of the Internet and mobile phone in which they operate. We should develop policy and programs that recognize and fund education and the development of new software tools. We should also guide and motivate the corporation startups and venture capitalists who build these amazing technologies.

I'm happy for tools like Twitter, that they can be used just as well to cover the daily lives of Ashton and Demi or break the news of Michael Jackson's death. But the fact that they can be used to broadcast updates from the streets of Iran or spread the news of political prisoners in Tibet being executed is a very weighty obligation and responsibility that they've taken on.

And last, we need to look at embargoes of technology and understand that when we embargo a country, we remove the possibility for the people that need these tools the most to have access to them. Thank you very much and my full statement's in the paper.

Mr. BROWNBACK. I want to recognize Congressman Bob Aderholt has joined as well. Bob, do you have a comment that you'd like to make?

Mr. ADERHOLT. Thank you, Senator. No, I just want to say it's good to have this hearing today and I'm glad to be here and to listen to our experts on this issue. It's an issue that certainly is, I think, the up and coming issue of the day. So thank you for having the hearing today and thanks everybody, pleased to be here.

Mr. BROWNBACK. Appreciate that. I'm going to have to slip out, shortly, for another meeting. I think this is a very important issue and we've got some funding coming forward in the appropriation bills to do some of the things that are being talked about here. But the accumulation of a policy record, I think, would be most helpful from the panelists and what you think it is that we ought to be doing and what we ought to focus on—both in the appropriation process and the authorization system. And so I welcome the record to be developed and to be able to use that. And with that I'm going to turn it back to Kyle to run the overall panel.

Mr. PARKER. Thank you very much, Senator, for joining us today. And we will continue with the discussion with Evgeny Morozov, who is Yahoo! Fellow at Georgetown University and contributing editor to Foreign Policy Journal. Evgeny?

Mr. MOROZOV. Hi. I'd like to thank the Commission for convening a hearing on such an important subject. While I share many of the recent enthusiasm about the positive role that new media can play in opening up authoritarian societies, I'm increasingly concerned with both how well some of the societies have themselves managed to adapt to the Internet threat and how poorly some of the digital activists, journalists and even some policy-makers understand the risks of trying to promote democracy via the Internet.

So let me outline some of my most pressing concerns today. First, you have to remember that new media will power all political forces, not just the forces we like. Many of the recent Western funding and media development efforts have been aimed at creating what's known as, new digital public spaces, on the assumption that these new digital spaces would enable the nascent actors or civil society to flourish on blogs, Twitter and social networks.

While this does sound reasonable in theory, in practice, we have to be prepared that groups that are often anti-democratic, both their nature and rhetoric, would probably benefit from existence of this net spaces as well. So in a sense, promoting this new digital spaces entails similar risks to promoting free elections. It's quite possible we may not like the guys who win. For example, research into the blogospheres in Egypt, Palestine, Russia suggest that these organizations like Muslim Brotherhood, Hamas, and various groups of Russian nationalists that are making the habits, use of blogs and social networks, in particular, because they are blocked from access to traditional spaces where they could operate.

So both support for promoting blogging and social networking may actually have a lot of negative and unpleasant consequences as well. Second, we have to realize that authoritarian governments themselves have developed extremely sophisticated strategies to control cyberspace and often those go beyond censorship. It's a mistake to believe that these governments wouldn't be able to manipulate these new public spaces with their own propaganda or use them to their own advantage. Many authoritarian governments are already paying bloggers and Internet commentators to spin the political discussions that they do not like.

It varies from the Russian approach, where the government is cooperating with several commercial startups which are creating ideological, social networking, and blogging sites that support the pro-Kremlin ideology. To the Chinese approach, where the party has created a decentralized network of what's come to be known as 50 Cent Party, which is almost 300,000 people who are being paid to leave comments onsite and blogs that the government doesn't like and thus, try to spin those discussions.

Even the Iranian clerics have been running blogging workshops, particularly aimed at controlling religious discourse targeting women. And they've been doing it, actually, since 2006, much before we began talking about the Twitter revolution. Third, authoritarian governments are increasingly eager to build short-term alliances with digital groups that sometimes their goals. For example, one of the reasons why Russia has emerged as the most feared player in the field of cyber warfare is because it always acts indirectly, usually by relying on numerous, nimble, underground gangs of cyber criminals.

Most of the time those gangs perfect the art of stealing credit card details of foreigners. But when the geopolitical pressures requires, they could be easily mobilized to assist the state. Just think of the recent cyber components to conflicts with Estonia and Georgia, with a communication networks of both countries have them crippled. Arguably, the fact that these networks of criminals who plan and execute these attacks rather than the government, actually, leaves Kremlin and Moscow more space for maneuver. So we have to remember that.

Another example, which I think is equally disturbing, is recent attempts to try to legitimize some of the Internet control by involving bloggers and Internet personalities themselves. For example, in the suggestion of the speaker of the upper chamber of the Russian Parliament, Kremlin may soon be creating what's known as the blogger's chamber, which will probably be another one of those state-controlled fake representatives of the civil society that will invite prominent Russian bloggers to set their own standards of what can and cannot be discussed on Russian blogs and on the Russian Internet, in general.

That's probably just another example where the supposed ceding of state power would probably only reinforce the Kremlin's control over the Internet. Fourth, we do not fully understand how new media affects civic engagement. And we don't have to pretend that we do. We still assume that established unfettered access to information is going to push people to learn the truths about human rights abuses or the crimes of the governments and thus make them more likely to become dissidents.

Most likely, lifting the censorship lid, at least in the short term, would result in people using this opportunity to fill in other gaps in their information vacuum. Those may have to do with religion, culture, socializing and so forth but not necessarily with political dissent. Political activism and active citizenship would probably only come last in this pyramid of cyber needs, if you will.

The creators of tools like Syphon and Tor which do allow anonymized access to the Web, often report that many users in authoritarian states actually use those tools to download pornography and access sites which that government doesn't want them to access—not necessarily political ones.

In fact, there is a growing risk that hundreds and thousands of these digital natives in these countries would actually be sucked into this endless cycle of entertainment, rather than have their political commitment increase and full political life. Finally, what I should mention is that current U.S. Government restrictions on the export of technology to sanctioned countries often actually thwart and impede the adoption of new media technologies.

I would like to point out that the current sanctions against governments like Cuba, Iran, North Korea, and several others make it significantly difficult for other ordinary citizens, as well as well established activists and NGOs, to take full advantage of the opportunities that the Internet and social media offers. American technology companies face fairly complicated process of obtaining and renewing licenses and waivers to be able to export their technology to the sanctioned countries.

The rules are not 100 percent clear and some technology companies decide not to take any risks and withdraw from this market altogether. For example, some American hosting companies refuse to deal with customers from Zimbabwe, Belarus or Iran altogether. And this inevitably leads to implicit censorship, where activist groups that actually supported

and were often recognized by the U.S. Government have to justify their activities to Web administrators of these companies. So I think I would stop here and you can turn to my full paper. I have two more additional points in it. Thank you.

Mr. PARKER. Thank you, Evgeny. We will now move on to Chris Spence who is Chief Technology Officer the National Democratic Institute. Chris, your statement?

Mr. SPENCE. Thank you, Mr. Chairman and distinguished members of the Commission. Thank you for this opportunity to comment on the role of new media in authoritarian states. For the last 15 years, NDI has employed technologies as components of many of our democracy strengthening programs. A wide range of technologies and associated strategies have been used to support activists, political parties, legislatures, women in politics, and civic groups around the world as the partners struggle to strengthen the democratic institutions in their country, increased space for broad participation in political life and safeguard their elections.

In this period we've been able to see the transformational potential of new technologies applied to democratic development. The new media and mobile technologies that have evolved over the last several years, while in many ways still exploratory in their application to politics, have been put to particularly good use in support of political campaigns and other forms of democratic expression.

But introduction of new media and other technologies should not be seen as a panacea for democratic development nor goal in and of itself. These technologies, paired with effective methodologies, can help organizations make significant contributions toward advancing the democratic process in authoritarian states.

Democratic development is a long-term commitment and a process. And the effective use of technologies by activists, political parties, candidates, civic groups and others can support and even accelerate the process when the tools are well used. Activists and civic groups have demonstrated remarkable ability to adapt new technologies and when combined with traditional organizing principles, can create moments of opportunity for democratic gains and enhanced channels for political engagement in authoritarian states.

The key is not only to employ effective technologies but to pair the technologies with strategies and approaches that are developed for the political environment in which the technologies are being used. This approach can help activists get out ahead of authoritarian regimes and make relative gains and even game-changing democratic gains when periods are identified where such innovations can rapidly be put to use.

While regimes may quickly catch up or clamp down by employing technologies and other techniques to bolster their regimes, gains made during the gap between early adoption and governmental response can have long-term, positive consequences for democratic activists. The strengths of the early uses of new media for activism have been in communication and in sharing information about political developments. However, thus far, we would argue that the tools have been less effectively utilized for the organizing required that can lead to constructive political outcomes.

In some situations, information has been produced by citizens using innovative new media tools that initiate the process of change, but the process is stalled due to a lack of the organizations or institutions in the country required to capture the interests and channel the process toward purposeful, strategic and peaceful direct action. Assisting organizations in these countries to build this capacity is an important component in leveraging new media tools toward political reform.

For example, those that followed the Iran election on Twitter may have felt frustration as a fantastic amount of information was captured and posted on the Internet during the election protests. But the pro-reform political organizations and institutions in the country were limited in their ability to channel the information and the energy of the crowds into a process that led to a reform based outcome.

One of the institutions that are particularly well-suited to this role, but often overlooked—sorry, I'll let that—

Mr. PARKER. It'll pass. [Laughter.]

Mr. SPENCE. How many—is that done?

Mr. PARKER. Something to do with voting in the House.

Mr. SPENCE. Great.

Mr. PARKER. Please continue.

Mr. SPENCE. One set of institutions that are particularly well-suited to this role but are often overlooked in international circles are political parties. Relatively little attention is paid to the important role that parties play in aggregating citizen interests and channeling them into constructive and peaceful means toward democratic reform. One area of opportunity, with tremendous potential in countries where NDI works, is to provide more new media technology assistance to political parties, especially in autocratic states where the regime often has access to considerable state resources and controls the organs of state communication.

NDI's work with domestic election monitoring groups provides an illustrative example of combining these new technologies with effective methodologies and strong organizations toward impactful, political purposes. A common approach to domestic election observing involves deploying citizen election observers, with their mobile phones, to a representative sample of polling stations around a country on Election Day.

These observers are trained to identify election irregularities or record observations and results. The observers transfer information from paper reporting reforms to a centralized national data base via text message or voice message. And the information is then aggregated and analyzed by the organizational leadership to make an assessment of the overall quality of the process, or accuracy of the election result. And then this information is shared with the public.

This approach is a way to collect substantial evidence to detect and deter fraud while building public trust in the process and adding legitimacy to election if things go well. The uses of these new media tools and related election activities have been very effective for our partners. Due to the rapid and accurate reporting provided by the tools and the data-driven analysis, this methodology has professionalized the way civic groups use quantitative election information in real-time on election day. And has been central to the ability of NDI partners to give the public a non-partisan view on the quality of the election process in their country.

In many cases, we believe our partners have made contributions that have prevented post-election violence or identified and raised important concerns about the electoral process that have led to more democratic and peaceful outcomes. The field of domestic election monitoring has improved significantly in the last several years, partly due to improved methods and strategies and certainly enabled by these new technologies and replicated by the role of international organizations.

Citizen reporting is another method by which citizens have been able to communicate various aspects of their Election Day experiences using new media tools, usually text messages and Tweets. The information reported by citizens is typically collected and made accessible to the public on a Web site or online map in raw form. The value of this approach is to increase citizen participation in the election process.

But to date, the challenge has been putting the information to good use. Tools are being developed to evaluate the authenticity and filter this incoming information so that organizations can then be prepared to put this powerful crowd-sourcing methodology to work during election periods. However, even as the tools and methods improve, citizen reporting promises to be a useful tool toward some electoral goals but won't be a substitute for election monitoring in situations where assessing the overall legitimacy of an election is required.

The last component of success for activists struggling for democratic reform involves the political environment in which they live and conduct their work. The challenges faced by activists in autocratic nations are immense. And these challenges are not only technical in nature but also legal and political. Authoritarian regimes typically put in place legal mechanisms such as laws that not only limit the activities of international and domestic NGOs and political parties but also subversion and libel laws against citizens who try to express their views and opinions online or publicly—laws against intermediaries of communication such as ISPs and telecommunications providers and legalized surveillance of citizens, including their online activity, and a wide range of technologies that they use to enforce these legal tools, including the Internet filtering and surveillance technologies that we'll be discussing today.

International community can help to create a more enabling environment for activists to utilize new media and tools in pursuit of democratic reform by implementing programs that foster greater access and affordability to technologies that seek more openness of these regimes, that advocate for increased freedom of expression and that protect the rights of privacy of citizens in these countries.

So to conclude and summarize, windows of opportunities for political reform can be created by the use of new media in authoritarian states with a combination of good technology tools, effective strategies and methodologies—put into use by organizations or institutions that can channel the energy of the public and the information they produce toward constructive and peaceful political activities.

The political environment provides the playing field under which all this occurs and we all have a role to play in creating an enabling environment, which activists and groups seeking democracy reform can work to build democratic societies without fear using new media tools. Thank you, Mr. Chairman and members of the committee.

Mr. PARKER. Thank you, Chris. We will now proceed to Shiyu Zhou, Deputy Director of the Global Internet Freedom Consortium for your statement.

Mr. ZHOU. Thank you. So the Internet is a vast, fast, and also inexpensive way to access information and to communicate. While authorities in closed societies can easily shut down newspapers, block TV channels, jam short-wave radios, and ban books, the Internet is far more elusive.

It has become the greatest hope for global information freedom and democratization and for peaceful progress of the sort the Helsinki Process made possible. On flip side, however, the Internet has also become the biggest target of information censorship for all

repressive governments who have put tremendous resources into beefing up their cyber war systems over the past decade.

The Internet censorship firewalls have become the 21st century Berlin Walls that separate our world. Amid the darkness of the Internet censorship in closed societies, a thread of light still remains. It is the Internet life lines offered by the anti-censorship systems like that of the Global Internet Freedom Consortium, GIF for short, which has been providing millions in closed societies for free access to the Internet for years.

GIF consists of small team of dedicated Chinese-American engineers who are brought together by a common practice of Falun Gong. Many of us were also among the students on Tiananmen Square during the 1989 massacre. Through the events of the Tiananmen massacre and the Falun Gong suppression, we have personally experienced how frightening the state controlled media can be. It confounds right with wrong overnight, inciting hatred in the society to pave the way for oppression.

It is our firm belief that free flow of information is the most effective and powerful way to peacefully transform a closed society and promote human rights and civil liberties. This conviction has driven us to spend countless sleepless nights contending with tens of thousands of Internet monitors and censors in China and around the world, so that the citizens inside those repressed countries may safely communicate with each other and with the world.

The men and women of GIF maintain operations out of own pockets but we provide our products and services to the citizens of closed societies entirely free of charge. After years of hard work, our anti-censorship system has attained global reach. It is used by people from almost every closed societies in the world and has been supporting the largest user bases in the world's most censored countries like China, Iran, and Burma.

During the Saffron Revolution in Burma, in late August 2007, we experienced the threefold increase in average daily traffic from Burma. Many Burmese use our system to post photos and videos of the crackdown to the outside blogs and Web sites. The Burmese government had to entirely shut down Internet to stop the outflow of information about the oppression.

Before the Beijing Olympics, when uprisings in Tibet led to thousands of arrests and large-scale human rights abuses, we saw our traffic from the region increased by over 400 percent in the first few days. Perhaps, the best example of the role of GIF software was during the Iranian election this past June, when our traffic from Iran increased by nearly 600 percent in 1 week.

On the Saturday of June 20th, an estimated 1 million Iranians used our system to visit previously censored Web sites such as Facebook, YouTube, Twitter, and Google. The Iranian users posted videos, photos and messages about the bloody crackdown. GIF systems have also been of benefit to U.S.-based organizations such as Human Rights in China, Voice of America and Radio Free Asia and even companies like Google and Yahoo!, who self-censor since we're bringing the uncensored version of their services to closed societies.

In fact, when the U.S. Internet companies are criticized for complying with the censorship demands of dictatorships, they often claim that they have few options but to do so. However, powerful anti-censorship systems make it effectively impossible for the regimes to demand censorship of those companies' in-country sites. This is because the more in-country sites compromise by censorship demands, the more likely people in those

countries will be to ignore them and to hook up to the uncensored overseas sites through anti-censorship systems.

The services GIF provides are invaluable and their impact goes far beyond the Internet. There are people in closed societies getting a taste of freedom and are given a way to share information. They will no longer acquiesce to tyranny and injustice. Internet freedom has the potential of transforming the closed societies in a peaceful but powerful way that must not be underestimated. The operation of our system is very efficient. It only needs a few dollars to support a user in closed societies for an entire year.

Moreover, for every dollar we spent, China and other censors will need to spend hundreds, perhaps thousands, of dollars to block us. The information warfare over the Internet has now boiled down to the battle of resources. We have technology and the commitment. With a modest amount of resources, there is capacity to tear down the 21st-century Berlin walls.

When Congress passed the Internet Freedom Provision in the fiscal year 2008 appropriation act, it declared that, quote, “ensuring the freedom of Internet communication in dictatorships and autocracies throughout the world is a high and critical national interest priority of the United States,” end quote. Thanks to this hearing and the bipartisan efforts now being made in Congress, I hope that the time has now come for the United States to make that priority come alive in a committed and robust fashion. Thank you.

Mr. PARKER. Thank you, Mr. Shiyu. We have one more panelist, who actually could not be with us physically today, Oleg Brega, who is a prominent Moldovan blogger who is actively involved in the post-election coverage and protest and demonstrations that took place in Chisinau. We do have, I believe, his written statement here available for the audience, as well currently on our Web site as well as our YouTube channel, which is just—I guess you go to YouTube/helsinkicommission, all one word; you should be able to find Mr. Brega’s presentation there that he did prepare for today’s hearing, and I would like to specifically thank Vlad Spanu and the Moldova Foundation for helping us out with that. We would love to have been able to telecon him in, or teleconference him in, but due to some logistical issues we weren’t able to do that.

With that, I’d like to thank the entire panel for your excellent statements and also for keeping to time. We now have a fair amount of time for questions, which I like to think are really the best part of these types of discussions. And again, we don’t need to limit you—the panelists can question other panelists or disagree, and certainly people from the audience. The only thing I would like to ask is if you could just keep your remarks in the form of a question and identify yourself. We do have a makeshift station over there, a microphone, and although we probably can all hear, it’s helpful if you do speak into the microphone for the benefit of the transcribers, who will transcribe your question for the written record of today’s event.

So with that, first to the audience, and we probably will take a few at a time and then let the panelists respond as appropriate. So sir, yeah, if you wouldn’t mind stepping up to the mic, and maybe we’ll take two or three to get it started and let the panel respond.

QUESTIONER. Good afternoon, my name’s Andrew Deming. I’m from the State Department and I’d like to thank the panel for holding this briefing today. My question was directed particularly at Mr. Spence, but any of you feel free, please, to answer it. I had the opportunity to observe the Moldovan elections earlier this year, and it was my first

observation mission, so I learned a lot, but one of the things I noticed was that a lot of the atrocities that would sort of make an election un-free or unfair sort of occurred in the months leading up to the elections.

And I really like the idea of using citizen observers and giving them the tools and technology to sort of go out there and report things on election day, but—and I know that they are the missions do go out there and observe any sort of foul play beforehand, but is there planning to do any activities or any ongoing activities right now to sort of utilize the same sort of strategy before the elections? Because I know a lot of the stuff doesn't happen on Election Day. Thank you.

Mr. PARKER. Do we have another question or two to sort of load the panel up here? Sir?

QUESTIONER. Thanks, I am Ben Bain. I'm a reporter with Federal Computer Week magazine. I was curious how important it is to avoid the appearance of interference. It was brought up a couple of times in the panel, but particularly with Iran, I mean, there was a lot of back-and-forth into what the appropriate role for the State Department was to play in interaction with Twitter and some of these other services, and I'm just curious about the take on how you avoid some of those concerns, and if it's important to in the first place. Thanks.

Mr. PARKER. One more?

QUESTIONER. My name's Robert Guerra, I'm the Project Director of Freedom House's global Internet freedom program. I have a question. There's the issue of measures and what specifically can be done, both from a technological point of view but also non-technological, human resource could be done, so there was specific comments on changes in legislation or others or hosting providers in the United States. It would be good to have a bit more details than were mentioned, but also the non-technical aspect that helps supplement opening up the Internet that could be useful to address the human skills that are needed. Thank you.

Mr. PARKER. Thank you. With that, please, maybe we can just start from this side to side, left to right or right to left, however you're looking at it. Please, Daniel?

Mr. CALINGAERT. Right. In answer to the first question, how do you gather information on pre-election violations? I think Chris made a very important point that it's not just the technology, but it has to be part of a larger strategy. And I think the same goes with [inaudible] for election monitoring or anything else. And so in principle, the same kind of technology that was used to get citizen input on Election Day can certainly be used in a pre-election period, provided you have the systems in place, and especially the people know about this opportunity and feed it in.

And there's a very critical component, also mentioned by Chris but often overlooked in these kinds of programs: The information needs to be verified. It is useless or even counterproductive to simply be passing around rumors, and rumor-mongering is very big in elections, and especially Election Day. So it's important as part of the structure that you have qualified people to sort through the information and call what is credible reporting from citizens from very unsubstantiated information.

In terms of the question about avoiding the appearance of interfering, the question on Iran, a lot has been said about the U.S. role. I mean, I think one of the most significant roles of the outside world was actually the diaspora community of Iranians, that a lot of the information got out via sort of personal networks to Iranians outside the country.

There were photographs from the days immediately following the election of Basij beating up student protesters and the like that might have been posted or passed around among a few people inside Iran, but they really only got—brought exposure because Iranians inside the country had friends or family outside who then would post that material on YouTube or elsewhere to get it broad exposure.

So the—Shiyu mentioned the importance of the anti-censorship technology. I mean, it was obviously critical that that technology was available and in fact in wide use within Iran so that there were—even though there were significant blocks on the Internet immediately following the June 12 elections, enough Iranians knew how to get around that to get the information out.

Mr. PARKER. Thanks. Please, yeah. And if any of the panelists don't have anything to say on a particular question, we can just move on. It just helps for everybody to have a shot.

Mr. FREITAS. I'll be terse. Regarding election monitoring, I want to just call out the Ushadihi—U-S-H-A-D-I-H-I. It's a crisis-mapping platform that has grown out of the movement in Africa after the Kenyan elections. It's akin to a blog system, but for mapping crisis, and what's unique about it is it allows you to capture unverified and verified information. So you—it starts to realize that just because something is tweeted, it's not true, and there's sort of posturing and deception. When we build systems that say, that is a type of data we'll have, let's figure out how to deal with it, you get something better.

And what's interesting, I think we've seen the first round, the 1.0 of a lot of this election monitoring. As these systems come in place, they'll be running all the time, and they'll be used in local elections and in state-level elections and the movement for—these tools will be easier, just like blogs. Everyone blogs; in a few years, everyone's got their own crisis-mapping platform.

I think in terms of avoiding interference, the role of groups developing proxy, amazing proxy software, independent activist groups, technologists, universities, these are groups that can kind of act without the national players getting involved, and that's the world I'm in, and in terms of the State Department asking Twitter to turn their servers off, that's a very interesting position that, where does it end? Do they keep asking more, can they change their SSL port so that Gmail is now accessible, do you just keep doing these things? I'm not sure.

And finally, in terms of what to do, I'll just give one example that I brought up in my opening statement—I think in the university system in the United States, we need to have more opportunities to educate students that they can have a career in using technology to support a variety of causes, and not just focus on Wall Street or going to work at Google. So I'm working on that, and I hope some of you will as well.

Mr. MOROZOV. I think the interference question is actually a very serious issue, and I think there is, more and more, a realization by many authoritarian leaders that there is a sustained effort by the U.S. Government and Western European governments and the foundations to try to undermine democracy via the Internet. Whether or not that is actually being made or not is a secondary issue.

And I think whatever the U.S. Government and its agencies can do to minimize that perception would actually be extremely useful. So from their perspective I think that reaching out to Twitter was the most terrible thing that the State Department could have done at that point, in part because it did confirm the thesis of David Inoshoradis that

Twitter is being used as a platform for fomenting the next revolution. And I think if certain things are done, at least, you know, it could at least be done privately.

But even beyond that, I think we see, now, looking at the trials happening in Tehran, that the authorities do perceive the information technology as a threat. Whether it is actually a threat or not doesn't really matter; they do think that Twitter and Facebook—and if you saw, you know, the trial of Kian, you know, the article in the New York Times yesterday, even the membership on the mailing list is already possibly an implication in being in some sort of spy network. So I think we do have to do a lot to minimize any kind of perception of interference.

So on the question of what's to be done, you know, looking broader than just what kind of laws we can pass and what we can do with companies, I think there is still an assumption that we have to go and start funding the creation of new digital networks and new websites and new blogs. And you know all of the media development has to change and to sort of target outputs and products to the media sector.

And as someone who has worked for a new media NGO trying to do some of that and who has advised some of the foundations on this, I can tell you that it doesn't really work that way in new media development the way it works, in old media development. You can't just go fund a project, wait for 2 or 3 years, and expect that it will either work or not, because in most of those projects, you know whether it is going to work or not in 2 or 3 weeks or 2 or 3 months.

So what happens is that because of all these bureaucratic models that we have, we keep waiting for 2 or 3 years. In the meantime, all of the people who could have been working on their own entrepreneurial projects lose any kind of entrepreneurial drive because they're all doing it either for the government or the government-funded NGOs, in those countries.

So my advice would be to actually focus on creating networks of people and focusing on conferences, exchanges, getting people out of Belarus, Turkmenistan, or Kazakhstan and hooking them up with bloggers in the Baltics, Central or Eastern Europe and then expecting them to go and create something, rather than just giving them, you know a check and expecting them to come up with the next Twitter because it's not realistic that, that's going to happen.

Mr. SPENCE. OK, I'll address a little bit of the election monitoring and the Moldova question to the best that I can. In terms of Moldova, in the July snap elections, I know that NDI was working with NMO—a regional international election monitoring group—and a domestic group. We had some problems and NMO was harassed and kicked out of the country and the NDI program largely shut down. We've seen a lot of positive changes in Moldova since then.

I don't have any information on our current program. I know that there was almost a Presidential election this week and that situation is a little bit fluid. And I don't have any information on our future programming in Moldova, although I would anticipate that we would support our domestic partners in very similar ways. In terms of addressing the long-term observing piece of that question, it's very, very common for domestic partners to conduct long-term observing, which is in the election period leading up to the election.

It isn't usually what makes the headlines on election day when we're making our statements, but almost always, whether we do an election-day observation or a long-term observation or both, we always do our best to capture what happened in the pre-election

period as part of our political statements about improving the process and coaching our partners on how to really take a look at that and include that in any statements that are made.

So pre-election period is very, very important, and whether we program around it or not and have the opportunity to work with partners in that period is something that's always considered. Media monitoring and other techniques are used to track election irregularities in the pre-election period.

In terms of the bigger question about election monitoring and the quality of data, one thing that I would say as a broad point—and I mentioned it briefly in the talk—is that the professionalization of civic groups in their election monitoring has really amplified and magnified in the last 3 or 4 years, and we attribute that to these tools.

Monitoring groups—and this kind of gets to the threshold questions about Ushahidi and some of the platforms where you're getting a lot of interesting information from citizens, but at the end of the day, you've really got to decide, have thresholds been reached which call into question the legitimacy of the process? And that's really the political question that election observers and the groups that we work with have to grapple with.

And there's so much involved in that methodology that one of the concerns about the crisis mapping or the crowdsourcing is that the public can then draw interpretations about the outcome of elections without necessarily having the filter required. You know, you can look at a map of some city and see 4 or 5 or 10 or several violations of election law reported by citizens who—you know, you have to deal with the verification problem—but is that significant in the big picture? If there's 110,000 polling stations in a country and you have a sort of a random grouping of reports, it's really dangerous to draw—it's a scale area to draw conclusions—about what conclusions can be drawn from irregularities that are reported.

So the observation process is a science, and the method of drawing those conclusions. And so it's really important that, as these tools get better—and we like the tools; Ushahidi and the other platforms are great—but we need to make a distinction between what can be expected out of a professional monitoring exercise and what can be drawn from unsolicited inputs from citizens. And I think there are good things that can be taken from both. I'll leave it there, I guess.

Mr. ZHOU. Yeah, I would just like to make one comment about this interference issue. So I guess it's mostly because of the State Department comment on Twitters, and I agree with Daniel that we should make the technologies available for the people in the closed societies. Whether we need to make that comment or not, that's a different issue. Because I am from one of such countries, so we understand the pain, you know, of the people in those societies. And they are very hungry for free information.

Just take this Iranian election as an example. So the usage—the traffic—coming from Iran on June 20th was so large and it soon consumed all our resources and crashed our servers. So we had to shut down the servers for maintenance—for cleaning—for a few hours. And we got so many messages and human phone calls from there. So when we restored the services, we somehow had to restrict the Iranian services, because otherwise our servers just cannot take that kind of traffic.

By accident, we curbed some of the video services because that consumes more bandwidth. And in particular, we stopped the YouTube services. And we got so much complaint from Iran and people even made calls to ask for YouTube service, so we restored that.

So from this, we can see that once we have this kind of tools available for the people, then you'll find and use it. We didn't do any promotion to Iran at all because, you know, we are a Chinese group; mostly we do Chinese Web sites and services. But they found our services by themselves and there were millions of users in Iran using this service.

So I think for a peaceful change in the closed societies, if we have the technologies available, whether it's Twitter, Google, Facebook, plus the anti-censorship systems, the people really will pick them up and that will be good for the society there. Thank you.

QUESTIONER. Hi, thank you for taking my question. My name is Matt Browner-Hamlin. I also serve on the board of Students for a Free Tibet, formerly with Nathan. My question is, going off of both the discussion of interference and dovetailing off of the third question about what can actually be done, I think the question of interference cuts both ways in that, while I think there's very clear consensus about how states should relate to technology in closed states, there isn't the same degree of consensus on how corporations, technology companies in countries like the United States can behave with authoritarian states.

And obviously, companies like Google, Cisco, Microsoft, and Yahoo! come to mind in the case of China, but there are many other less prominent examples that are probably even more pervasive in terms of the impact of speech within a closed society. So I wonder what can be done specifically in the United States relating to the behavior of American technology companies toward authoritarian states and their products. Thank you.

QUESTIONER. Hi, I'm a program officer at the Academy for Educational Development, and I've been managing civil society program in Moldova, now, going into the third year.

Mr. PARKER. And what is your name?

QUESTIONER. Kristen Farthing. I was very excited by the events in April and they continued to the summer with the re-election in August. And my question is how, as a development professional, managing programs, how can you channel that energy and sustain the protest in a way that then becomes a concerted political action by youth?

Mr. PARKER. We'll take one more and then we'll take two more, if we have them.

QUESTIONER. Hi, my name is Mark Palinsky with Digital Democracy. There's a sort of lumping of tools under one, sort of, big header—this new media tools. But each tool is different, whether it's Facebook or Twitter, and the responsibility that each tool sort of takes onto themselves for the security and privacy of their users is also different in each specific case. So I'm curious if there are tools or methods that you would encourage—whether open-source or otherwise—that we really start to focus on, contra other tools that might be good for social networking but, particularly under authoritarian regimes, can be really dangerous because it doesn't protect the individual users.

QUESTIONER. Hello, my name's Will DeKerna. I'm with the State Department. I guess my question builds off the second question, here. You mentioned how important it is to couple the impact of these new technologies with the institutions—the political parties that are needed to make that into real change. And I'd really just like to hear any of the ideas any of the panelists have about how you can do that, given, I feel, the room to operate for information technology is often much greater than to deal with political organizations and things that the regimes are more afraid of than the technology itself, and how the panelists feel you might reconcile that gap.

Mr. PARKER. Thank you. With that, we have, certainly, more than enough to begin responding. And why don't we start from this side with Zhou, if you would like to respond first.

Mr. ZHOU. So I would just make a comment on the third question, about the open-source and security issue. So you know, for Twitter and Facebook and YouTube, those kinds of services, it's very different from the anti-censorship services. Those services are basically a kind of service provided, you know, for whether it's in the closed society or in the free society for public use. So for that, of course, there are privacy issues; there are security issues and others. But it's not as acute as for anti-censorship technologies.

For anti-censorship technologies, you know, we're basically being attacked, traced and reverse engineered and studied extensively and fiercely by the censors. And so the user safety is the biggest priority of ours. Also we have to penetrate the firewall. We have to enable the users to pass through the firewall censorship safely.

So for that, it's a problem that there are certain technologies that do not work well and that has potential big problems. We do not want to address the details of the technology here, but we do have such issues. But for the technology like ours, for example, it's been working quite well because, you know, if we can protect the people—especially those dissidents in China—pretty much, we can protect everybody in the world. But it does need a lot of work so it's not an easy job.

Mr. SPENCE. OK, let's see—the question about how to channel the energy. What are the strategies and methods that are used to take the information that's coming out of these new media tools and put it to productive use? And I think that there's a whole lot of ways to get at this, and one thing I would say generally is, it's political-environment-contextual. So you have to sort of build the solutions based on the political environment you're working in—the relationships in the country, the politics of the country and some of these other constraints around security and safety of your partners.

One of the tried-and-true ways that we do it at NDI is work through NGOs and political parties that are reputable and have the public trust of the citizens. So as the information comes through these channels, it can be looked at, it can be reviewed, it can be analyzed. And then someone can get on television or get on the Web or get wherever they need to get to and say things that are useful and practical for the citizens to sort of act upon.

And the idea here is, in a lot of situations for us, it's try to form your statements in ways that prevent violence, that talk about using legal channels to vent your frustrations. There's often a judicial or some sort of adjudication process. And really, in these activist environments, it's really important that the message is, identify the legal channels, use them, use partners that people can identify with and trust so that they can take the lead from those kinds of partners.

You know, if you look at what the Obama campaign did, you know, there are all kinds of strategies that you can look at depending on, you know, the environment, and books are being written on all those that are relevant to the U.S. political scene. But generally speaking, it's context-specific and it's really not—it doesn't have to be rocket science. Just get good people who understand the environment to design the programs.

In terms of tools, you know, the ones that NDI partners use are the ones we're talking about. Skype is huge. Skype is a really important technology. I don't know if it sort of meets the threshold of new media, but it's very important. It's relatively secure

and it's easy to use and it's cheap or free. The Tor and the GFI technologies and you know, all of these onion routing-type things are important.

I don't have a firsthand knowledge of how much our partners use those. I think they are important in some countries, and certainly, widely utilized, especially in these mass movements. And then there are, of course, Facebook and Twitter. So the strategies differ from tool to tool, but I would think those are the ones that I would say we think about and we see people using.

And I think I addressed the two questions. I guess I'll call it quits. Did I address your question?

QUESTIONER. More or less, I was just interested in knowing what happens when a country kind of lets outsiders come in [inaudible] increase access to technology but doesn't allow anyone to interfere with the political process [inaudible]. And how do you get around that? So I just [inaudible].

Mr. SPENCE. Well, I guess we're talking about the tools and strategies around that. I guess what I would say is that whenever activists are in these countries and they're getting ready to think about decisions about using these tools and their own personal safety is at risk, what NDI would do is, to the best of our ability, coach on the parameters of the tools and how they might be used and what the risks are. And then everybody is going to have to make a personal decision about how they're going to use the tool.

In a lot of ways, the Internet tools that we're talking about are black boxes to a lot of people. They don't know if, OK, I've got this image on a phone or got this video on a phone, what am I going to do now? I have a decision to make. Is it safe for me to transfer it? Is it safe for me to put it up on YouTube? You know, how am I connecting to the Internet? All of those decisions have to be made on a very personal level and I think that's one part of the discussion that gets a little bit missed, when you think about these people using these tools.

It's easy for us to sit around and talk about using the tools, but if you're in that position where, you know, you can see the riot police coming at you, you can see the stones and you make those decisions as an activist—but if you have to sort of deal with the technology and it's a bit of a black box, those decisions are hard. And activists around the world will have to deal with that challenge.

Mr. MOROZOV. I think I'll tackle the question about companies—investment companies, more specifically. First, I think we tend to lump different corporate activities together here. I mean, first you do have companies which provide technology for monitoring of traffic and surveillance and censorship. And then you have companies who provide basic services, like e-mail or social networking, and under pressure, may actually disclose the personal details of their users.

And I think we should [inaudible] too, because it's important to understand that a certain category—you know, provision of services—if we antagonize or, you know, sort of push Western companies from this [inaudible] to this market, their places will be quickly taken by the local companies, who often are much easier to manipulate and actually pressure and are releasing all sorts of personal details.

So while we may think that Google mail or Yahoo! mail are terrible and those companies—but the government—I'm not sure that they are that worse, ethically, than the majority of the companies in China, who probably often do that without even disclosing it to the media. So we have to make sure that we do not necessarily, you know, push the

Western companies out and ensure that the locals take their place, because they would probably be much easier to manipulate. I mean, if you look at censorship on Chinese blogs, Chinese Web platforms are, increasingly, very eager to self-censor.

I mean, research by Rebecca McKinnon last year showed that when she went and created controversial content on dozens of Chinese blog platforms, her content disappeared within 24 hours from most of them, right? And it's considered normal by their standards. If you had that page pulled from BlogSpot or MySpace, it would probably be a scandal of international proportions.

That said, the first category—the companies which do provide technology for filtering and surveillance—I think they would be much harder to replace, yet, by domestic competition because some of that technology is fairly sophisticated. Even there, if you look at how the Chinese tried to implement the Green Dam censorship package that put a limit to what you can do on your computer, you actually see that they did steal some of the technology, apparently, from Western companies.

I do think that even if we try to limit what the Western companies are doing, you'll still have some of that knowledge already out there, and the locals, particularly paid or funded by the government, will build on that. But that said, I think the crucial question here is transparency. And that's a question of whether we have to do it through some legal norms by requiring companies that do export any sort of technology to those countries to disclose exactly what it is.

At this point, I'm still not sure whether or not Nokia-Siemens is supplying any packet-inspection technology to Iran despite, probably, a dozen press releases from them, right? And I think we do have to achieve a standard under which we do actually know what's going on. And then, you know, I expect civil society and the NGOs will actually step in and try to mobilize boycotts or protests, just like they do against other corporations who engage in unethical practices. So I think I'll just—

Mr. FREITAS. I would like to actually point out there were domestic versions of Twitter that were created in China that actually haven't lasted, and now they've been shut down entirely. So there are some strange cases where this does happen—where someone says, we'll make the Chinese Twitter—and maybe it's—you can't even censor it, you know; it just gets completely turned off.

I think there's another class of technology that has emerged, which is sort of the camera-surveillance technology. What's interesting about that is, it's sort of globally accepted in this war on terror—you know, I live in New York downtown and I understand why we want surveillance cameras. I understand why London wants surveillance cameras. When authoritarian regimes get the power of surveillance cameras and they can decide who are domestic terrorists—you know, Tibetans are terrorists; the Uighurs are terrorists—you know, the power of that is scary.

And Naomi Klein wrote a great article looking at Shenzhen and Lhasa and some of the areas in China with surveillance camera and image recognition and things like that.

In terms of channeling energy, I think a lot of my work is looking at connecting non-violence practice with new technology. And I think about, how do I know who Lech Walesa was, thinking that he said let's not charge down and take to the streets; let's sit in this factory and work the phones and work the media and the press and sue these communication tools to get our story out. And that kind of thought process and, in the new media age, needs to be encouraged.

So looking at, again, something like the Alive in Baghdad or numerous other projects that use social media tools to create citizen-journalists out of people that might otherwise be frustrated rioters, so to speak. So I would call to the news media organizations to look at working with local citizen-journalists on the ground instead of sending in your correspondent—your embedded correspondent.

Finally, Skype is a great tool. And it's an interesting trend in telephony, in which, our phones are becoming more and more virtual. You know, Google Voice is the latest craze. You know the phone system is becoming this very malleable, open-source thing where, during—you know, in some work I've done, I've set up banks and banks and banks of virtual phone numbers that all go to the same line so that you can't trace the person by the phone number that they call. And you could change; you could have a hundred new phone numbers a day. There are things you can do with the phones that are amazing that are what we think of the Web, we're going to start thinking of with the telephone. So keep an eye on that.

Mr. CALINGAERT. I'd like to add some comments on the question about U.S. companies. Obviously, there are efforts through the global network initiative for the companies to raise their own standards on human rights issues, and in collaboration with the human rights organizations. And my sense is that will only take them so far.

And part of the problem, even in that initiative, is that it's currently limited to three companies and it doesn't include Web 2.0 companies and it doesn't include any foreign companies. And I think if there's going to be discussion about raising the human rights standards of companies, we should not just be looking at United States, but also European, Japanese, and other companies working or based in democratic countries.

Obviously, Evgeny's distinction, I think, is very good between those who are providing basic services and can be more easily replaced by local companies in China or elsewhere, versus those who are developing technology. I think we need to do a lot more regarding the companies that produce censorship and surveillance technology.

And you know, the Nokia-Siemens case—you know, obviously more information is needed, but it looks pretty clear that they exported a surveillance system which would be pretty standard in any country, but the fact that it's in Iran strongly implies that it's used to track down peaceful dissidents. And you know, similarly, there are indications—not enough research, but strong indications—that a lot of the censorship technology used in the Middle East is basic sort of Net Nanny software that is used in the United States and elsewhere.

And again, you can use it in the United States, where we have legal safeguards and court systems and protections for individuals; if you take that into countries where you don't have rule of law, chances are pretty good it's going to be used to censor political content and criticism of the government and the kind of free speech that we ought to encourage. And so I think this is an issue that really requires some government action.

Mr. PARKER. Thank you. Please.

QUESTIONER. Hi, Erica Moratt from Voice of America, Russian Service. And I have one question to whoever wants to answer and one to Evgeny Morozov. First question—I'm going to use the buzzword terrorists, but this also includes criminals and organized criminals and groups—to what extent can they use those open sources? Because I mean, you know, Osama bin Laden can't have a Twitter because obviously he's going to be tracked.

And my second question is to Evgeny Morozov: Russia has invented Gogul search engine, allegedly for kids, but it does figure what information you can search. Do you see it as one of the tools to censor Internet, or it's just another search engine? Thank you.

Mr. MOROZOV. I can start the second question. I mean, those efforts are pretty common, particularly in Western Europe now, where there is a strong push to make the Internet safe for kids and to make sure that it's safe from child pornography.

And I think the bigger problem that I see with this current rhetoric is that we need to start blocking access to those Web sites is that people who really want to access them still access them, because what's happening is, we are not eliminating the content; we are not going after the actual sites. We are just preventing access to them. So the content is still there. If you're really smart, you can actually figure out how to access them.

What I see as the downside here is that you get more and more countries—Russia and China included—who point to the West and say that look, guys, you are having your own campaigns to limit freedoms online, whether it's because of child pornography or something else; why aren't we allowed to do the same in the same fields, or maybe in the field of politics.

There was a crackdown on pornography earlier this year in China where they blocked several thousand Web sites. And at least several of them were not exactly clear-cut cases of pornography; you could actually make a case that several of them were sites which write about culture and often write about sensitive problems for the country. And the fact that, now, we see more and more crackdowns like this, sort of, or often this rhetoric of, let's keep the children free, is a little bit terrifying. And I think that, at root, it's not very effective because the real criminals are still using those networks.

And to your first question about terrorists and who else is using the Web, I mean, it doesn't make sense for any group which wants to remain invisible and unseen and which doesn't have any resources to organize and mobilize to use the Web—first, to communicate and then to do outreach. So of course it's happening. But the question is, how do you define terrorists, first, right? And then exactly, are they going to be more powerful than people fighting for freedom? And here, it's not a question of technology; it's a question of politics and social forces. So I don't think we should stop promoting those tools simply because terrorists are going to use them because you know, that would simply be counterproductive.

Mr. FREITAS. I get asked this question a lot as well because I'm building, like, an encrypted phone and people are like oh man, the Mafia is going to love that, or something. So it is—and my students ask me this as well—and I don't, from an engineer perspective, I don't want to be the guy that said yeah, just, I made the AK-47 and you know, it's a great gun. [Laughter.] So you have to be careful. You need to inject morality into these things, but it's a slippery slope.

So I think ultimately, the use of tools for positive gains outweighs them for criminal. And criminals already have plenty of tools at their disposal for corruption and money laundering and things.

Mr. PARKER. Any other questions?

QUESTIONER. Might I ask a followup on that topic?

Mr. PARKER. Please, Neil. Neil Simon with the—

QUESTIONER. I'm sorry; I should go to the microphone. I'm Neil Simon. I am the Communications Director for the Commission, but I want to followup on that question,

looking at who is more developed right now in the use of this technology. And we've seen a lot of great examples from civil society, but are terrorists and other negative groups more advanced, in some countries, than even civil society and activists? We see this in, you know, border drug wars and whatnot. We always see people getting a step ahead of law enforcement; do we see the other side getting a step ahead of activists?

Mr. MOROZOV. I mean, I can answer it quickly. The problem is, we never see the most successful acts of either activism or terrorism online because if you really want to be effective, the last thing you want to do is to publicize your networks. And that's why I've been somewhat skeptical in the ability of Facebook and Twitter to be very useful in planning and organizing a revolution, because those platforms, by default, are open to anyone.

You know, they're open to anyone to watch. And probably, they can be very useful in publicizing what has already been planned, but they are extremely visible. And there are a lot of people on both sides who actually would want to watch them. So I think we, and analysts of this technology, are always one step behind because the moment technology attracts attention and becomes public, it stops being useful for people who are actually using it.

I'll give you an interesting example. You know, Iranian activists used to conceal and hide their political discussions on a social networking site for book lovers called Goodreads. And you know, a lot of people use it for purposes that have nothing to do with Iranian politics, and that was the whole point, that you can actually carve out a little space on that site and actually carry on the discussions and people seeing—the Iranian secret services—would never guess that those discussions are going on. Now, the moment the Los Angeles Times published an article about it, I'm sure it stopped being useful, right, so they had to move on somewhere else.

So that's the tension that I have, for example, as an analyst: Even if you know the tools are being used, to what extent can you disclose that they are actually being successful? So it's very hard to answer that, in short.

Mr. ZHOU. I want to make a comment on this terrorist issue because I've been asked similar questions many times. So there is a difference between anonymization tools, which I believe some of us mentioned, and also, anti-censorship tools. There is a difference between those two concepts. Anonymization tools, I would say—let's not be so absolute—but almost all the other tools except ours are anonymization tools. And they're used for, mostly, communications that hide the user's identity. And they cannot be used with targeted blockage by the censors. So in other words, if a censor wants to target this to the target and tries to trace—you know, break the security, then there is a potential danger for them to succeed.

Anti-censorship tool is to use in the hostile environment that is targeted by the censors. So they know your tool and they know where your proxies are and try to block you. So in other words, it's used for a massive effort to bring down the firewall. And the other tools are mostly for private use and small-scale use and are unscalable in a lot of senses. And for those kinds of anonymization tools, indeed, it is possible for misuse, frankly speaking.

But for our tools in particular—the anti-censorship tools—it's probably the last choice for terrorists to use. It's because their encryption is only between the users in the censored countries to the proxy server, but once you get to the proxy server, you get, from proxy server to the destination is completely open. So it's just like using the normal Inter-

net. So they can do anything in the, so there is no advantage for using our tools for the terrorists. So it's just like using the usual Internet. So there is a difference between those two concepts.

QUESTIONER. Hi, I'm Emily from Digital Democracy. One thing that I heard emerging, which is something that I think is really important, is the idea of how citizen-journalists, how activists, can learn how the different new media tools can be used and how to use them effectively—so what I would call new media literacy.

Just as media literacy was critical to the 20th century, I think new media literacy is critical to the 21st. And I'm curious if you can share any case studies of, maybe, how people on the ground have learned how to use the correct tools and use them effectively, particularly in terms of addressing security concerns.

Mr. PARKER. Thank you. And I'd also just like to possibly add to that question a question of mine: Again, the notion of, you have these tools available—the very nature of these tools—they're things we couldn't have thought about years ago. And there's the assumption that anything's possible and who knows where we'll be in a few years. So if somebody gives me a flash drive preloaded with Tor or something and I'm a civil society activist in Ashkabad and they say I can browse the Internet or communicate or send e-mail to people in Washington or friends in Europe or whatever safely, how do I have the confidence? And how do I know that—you know, some of it's like, well, I can put a really serious lock on my door but if my door is a pinewood door, then the lock doesn't have to be broken; you just break the door.

Or if I have an encryption key that's very serious but the stick-it is right there, or someone's in the room with me in an Internet cafe or, who knows, is there an internal camera in the computer keystroke monitoring? And it seems like, how fast this technology changes, can the end user, who's not a computer nerd or whatever—or geek or whatever—somebody who's really technical about this, but a simple—someone's who's someone else—a journalist, a citizen. Can it ever get to the point where there's adequate confidence, particularly in societies where the price or being discovered can be serious? It could be prison. It could be worse. And I think that's part of illiteracy as well, and can you sort of round that square or whatever? How do you address that?

Mr. CALINGAERT. Yeah, it's a very critical issue. And let me put it this way: Freedom House works with activists in many repressive environments and I can think of at least a couple cases—well, several—with activists from very repressive environments who were very sophisticated as activists and they were, frankly, very naive about the security of their online communications.

And there was one in particular who, her e-mail was tracked and it turned out that her e-mail was literally `firstname.lastname@yahoo.com`. So things that we would find pretty obvious aren't necessarily that obvious to even, sophisticated activists. And you know, we're talking about the basics in this example. I mean, once you get into using different anti-censorship tools or Tor or you know, Hushmail, Vaultlet—those kinds of things—it takes training, frankly. I mean, there probably are some users in places like Iran or Saudi Arabia or wherever who can kind of learn it themselves, but in many cases, they're more likely to learn it if they come into, let's say, face-to-face contact with people who understand it and can explain it to them.

Mr. FREITAS. I've learned an important lesson in working with the Tibetan independence movement and others: It's that we can't presume what people are willing—are or are

not willing to do for their own freedom and liberty and democracy. We can't say, oh, if they do that, they might get arrested or go to jail or get killed and we can't do that. These are people, as we saw in Iran, who are willing to take to the streets and die for their freedom, and you know, it's an important fact to remember to not presume that you want to protect them.

As far as a case study, a good friend of mine is part of TextPower in the Philippines. And I really like this model because it's very simple. Tony Okruse is his name, but there's a whole group of people in the Philippines that have used text messaging not to go to Twitter, or the Internet—not to be centralized. We get so caught up on having all these people out here texting to the middle and going back out.

What they figured out in the Philippines is, this is about your phone going to other phones going to other phones; you know, this is kind of edges and use of messaging built on top of the constructs of society, and using what they already knew how to do. Like everyone in the Philippines knows how to take a text and forward it to their address book. So they used that technique, as opposed to forcing new behavior and saying, oh, what you should use is Twitter. You know, when Twitter came out in the Philippines, it wasn't a big deal, and they said, well, why should we use that? It's centralized. So I think there are cases where you look at the behavior of what users are already doing and help them do it better.

Mr. MOROZOV. Well, I think the question of literacy is actually very important, and I think there should be more ways to train activists not only in the use of tool, but also raise awareness about the vulnerabilities and risks that even such basic activities as social networking, for example, bring, even if you are perfectly anonymous. If you do have accounts on several social networks, for example, but just overlapping those different social networks, you actually can learn quite a lot, if not about yourself than about people in your networks.

It is actually a little [inaudible] security research going into this question of the social graph, right? And there are scientific studies which do prove that you can glean a lot of information simply by overlapping the presence of people on various sites like Flickr or YouTube or Facebook, right? So I want to make sure that activists have heard that, right? They think that just because I use Tor, just because I use Gmail I'm untraceable, right? And in that sense, they don't realize that by joining any of the Web 2.0 Web sites, they kind of give up part of their anonymity and they give up part of their sovereignty or whatever you want to call it, and I'm not sure they realize that.

The second point I want to make here is that there will always be the human factor involved here, and you would never, no matter how secure your technology is and no matter how many trainings you run, you still run into basic problems, particularly in authoritarian regimes, where torture is much cheaper than hacking. It is much cheaper to go and torture an activist and asking for his passport than to hire 10 hackers, who will then go and crack his inbox, right? And as long as that's the case, I think we can be building all sorts of tools, but the reality on the ground will be that, well, either you stamp out the e-mail and your e-mail inbox self-explodes in 2 weeks or you just act more securely.

So I feel these emerging threats are not yet fully understood, and I think we need to start looking into them and sort of going beyond these tools discussions that we've been having.

Mr. SPENCE. I would just add a couple quick things. On the library toolkit question, I think absolutely. We think that the tools are evolving, and they're generally moving in the direction of easy to use and easy to sort of get your head around. So the strategies are what it's all about. It's about identifying the levers of power in a country, understanding the political environment, the law, the legislative process, et cetera, et cetera and then designing strategies, using toolkits if you can to sort of get the general idea, and then designing strategies that can effect change using those levers.

And so yeah, so absolutely, and then you have to find good partners in these countries who can really sort of get their head around this and move it forward, and I think those are the keys to success. On the question of confidentiality and anonymity, I think we, or at least me and my team, we're pretty conservative on this with our staff and our partners. I generally sort of use the analogy of locking the doors but leaving the windows open, similar to what Kyle was saying. The technologies—you're never very—all that certain how secure you're going to be.

We think our real vulnerabilities are in our physical offices, where people print something off the Internet or they download something or they have cookies on their machine or they do any number of things, and when NDI finds itself in difficult situations, it's usually—an unfriendly knocking at the door—it's usually not some kind of a surveillance—especially—surveillancing technology—especially in countries that aren't as—China and Russia, absolutely, that's an issue, but a lot of the smaller countries with less resources, we really view our vulnerabilities and the vulnerabilities of our partners in this issue related to how they choose to use the information that they happened to find on the web, and leaving paper in the trash, and all the more obvious things. So do that first and then think about the technical things.

Mr. ZHOU. Just to make a quick comment about Kyle's saying that, indeed, for a lot of users in closed societies, they are not sophisticated or computer-savvy users. So from my experience over the past, for a computer-savvy user to get around a firewall is not difficult at all, because all the circumvention ideas are based upon the proxy-server idea. So as long as you can find like a—for example, I'm in Beijing, I want to go to cnn.com, I cannot go. I find a third-party, called proxy, server in the free country and hook to that, and that's like a detour, and that server can get information from CNN and pass it to me. So that's the basic fundamental idea of circumvention. So even for the computer-savvy user, this is not a hard thing for them to do at all. So for a small-scale operation to penetrate firewall is—it has the existings when the Internet started, so it's widely used for—in the computer circle, the computer scientist circle.

However, so what we are talking about now is to make a decisive and massive effort to tear down the wall. So that is, for any user, an every-day user has no computer knowledge at all, even. As long as he knows how to get Internet, then he can use the little tool and double-click it, and then he can penetrate the firewall. So that's the very, very challenging work. So that's the—first of all YouTube needs to be designed specifically for the computer ignorant users, and also has to protect their safety. So that's the work that we are aiming at.

Mr. PARKER. Well, we've come to the end of our time today. It's obvious we intended this to sort of be a survey discussion. There's so many facets of this, I can see us exploring further the technical side, sort of a how-to, what's available, the state-of-the-art, sort of a cookbook for activists and citizens, the policy side, addressing the issue of terrorists

using these technologies or other questions, and then hearing from people who'd really put this to use on the ground, sort of the pragmatic.

So I can see that we will be discussing this further, and like I said, this will be published and become an official government product, and when we had the idea to do this, we looked in CRS, in Congressional Research Service, no readymade product on it. As far as I can tell, there has been no other congressional hearing specifically on this yet, and I expect that all to change. In the coming future, there'll be a lot as there's a lot of pending legislation. So it's certainly something this particular audience here on the Hill is very interested in and we will continue to discuss.

I'd like to thank the audience and all of you for the questions, for coming today. To our distinguished panel, for your excellent presentations and all the work you're doing, and also to Chris Doughton and Max Duiz for basically putting this event together, and I'd like to thank you all also for putting up with the uncivilized buzzers that we have. It sort of comes with the venue, but with that we'll adjourn the discussion here.

[Whereupon, at 3:54 p.m., the briefing ended.]

# APPENDICES

## **PREPARED STATEMENT OF NATHAN FREITAS, ADJUNCT PROFESSOR, NYU INTERACTIVE TELECOM PROGRAM**

I greatly appreciate the opportunity to participate in this hearing.

Thank you to the members of the commission, Chairman Cardin and Co-Chairman Hastings, for the invitation to appear here today, and for your interest in this very important topic. I come to you as a representative of the countless technology and new media advocates, experts and educators who believe that the most amazing and ground-breaking innovations of our generation should be used for more than just the acquisition of wealth or as new channels of entertainment and distraction. I am also a longtime member and former board chair of the international non-profit group Students for a Free Tibet, led by Tibetan activists Lhadon Tethong and Tenzin Dorjee. What I will share with you today are some of my experiences working with new media technology as an activist practitioner, and my ground-level perspective, so to speak.

First, a small bit of history. The roots of this latest wave of new media technology, specifically Twitter, began in 2004, with an open-source web service called TXTMob. TXTMob was first developed by MIT's Institute for Applied Autonomy for use by protesters at the 2004 Democratic National Convention in Boston and the Republican National Convention in New York. I was part of a team that utilized TXTMob to broadcast thousands of short messages to over 10,000 people on the streets of New York, letting them know what was happening moment by moment. Later in 2004, during the Orange Revolution in the Ukraine, students utilized the same service to coordinate spontaneous protests also known as "flashmobs", strikes and sit-ins. In 2005, two of my colleagues who had been involved in TXTMobs use during the RNC went to work for the company that became Twitter, where they demonstrated the power of short message broadcasting to their coworkers around the office. It was in those times and in those moments, that the idea for Twitter was born. It is not an accident that things have come full circle, with Twitter now being the standard go-to tool for activists around the world.

In my activism work, my areas of focus and expertise is Asia. I have specific experience traveling in and working with organizations focused on China, Tibet and India. I have also been employed in Silicon Valley and Silicon Alley, developing patented technology focused on the exchange of data between mobile devices over wireless networks. As a student at the University of California in the mid 90s, I worked on a DARPA and NSF-funded research effort known as the Digital Library Initiative. Today I am an instructor at New York University's Interactive Telecommunications Program, teaching a new graduate course entitled "Social Activism using Mobile Technology".

My personal path in this sphere, as a developer, practitioner and instructor in the use of new media technologies within social movements, may seem novel, but is in fact built upon a very long tradition of geeks trying to good.

During the second world war Second World War and the Cold War, inventors, mathematicians and the earliest digital computers played a critical role in helping the allies stay one step ahead of the axis.

During the civil rights movement, the use of telephones, telegrams and traditional social networks within churches and universities, helped build a foundation to mobilize supporters throughout the south. In recent years, open-source hackers, nerds and geeks

have gravitated towards the social justice, environmental and human rights movements, creating unique alliances and very rich opportunity for innovation.

The idea of two guys in a garage in Silicon Valley has translated into global teams of activists communicating in realtime through Twitter, Skype, Facebook through their laptops, iPhones and Blackberries, working to weave together the grassroots organizing and non-violence tactics of Gandhi with freely available, open-source software, cheap internet bandwidth, cloud servers and mobile devices.

Take the case of Burma in 2007. Video journalists and I.T. (Internet technology) student organizations teamed up to provide their own coverage of the Saffron Revolution. Using SMS, instant messaging technology, digital video cameras, internet-based file transfer services, combined with old fashioned “sneaker nets”, a network was able to present an uncensored view of the protests as they unfolded.

As their footage began reaching the outside world, appearing on the BBC and elsewhere, the journalists became more bold and increasingly targeted by the state security forces. When the revolution never fully materialized, the monks, activists and journalists involved paid a very heavy price, facing imprisonment, torture or worse. However, the innovative work of the video journalist teams made a lasting impact and was largely considered to have been successful due to the global attention the protests received. A similar model is being used in Iraq, through the award-winning online video channel, “Alive in Baghdad”, that works to cover and disseminate stories of the every day lives of Iraqis. We have also seen this model used with simple camera phones in the Kashmir and most recently in Iran, when a single video clip of video of an innocent dying girl instantly clarified the issue for a global audience and brought overwhelming sympathy and support to the side of the Iranian people. The power of the moving image is unavoidable, and with the low cost of distributing video online, the ability to easily stream live over mobile and satellite data networks, its reach and impact has come to rival broadcast television.

In many cases, the authoritarian states’ power proves too formidable for new media technology to have a meaningful impact. While we can instantly know about the smallest conflict in any part of the planet, there is often very little that the Internet can do to help those in harms way. In Tibet, the largely peaceful uprisings in March 2008, were perceived by the outside world as being “riots”, due to China’s ability to control the story by severely restricting news media access and blocking telephone and internet communication. Thousands of Tibetans were detained, many died, and hundreds were given lengthy sentences, many convicted through evidence gathered via close-circuit security cameras, use of mobile phones, PCs and the Internet. Just yesterday, four Tibetan political prisoners were executed after being hastily convicted of crimes related to the March uprising. There are countless stories of Chinese, Tibetan and other activists within China being incriminated through their use of email, Skype and other tools.

The evidence gathered by the state is often done in collaboration with the technology providers—Yahoo!, eBay/Skype, and so on.

In August of 2008, over seventy activists from around the world traveled to Beijing to protest for Tibetan human rights and independence during the Olympic games. New media tools played a major role during this effort, providing a loosely coupled link between the various independent activists who were traveling to Beijing to participate in protests. The tools also enabled a team of citizen journalists to document the many different protests and press conferences that occurred, using techniques evolved from what the Burmese students accomplished in 2007 and a bevy of new technology—solid-state HD

digital video cameras, handheld tablet computers, live streaming camera phones. Their photos and footage were broadcast around the world, appearing in the NY Times and on the BBC and CNN International. Mainstream press was unable to cover the majority of these events due to the close monitoring and scrutiny they faced. The Beijing authorities eventually caught on, arresting and detaining for a week, six American citizens who had been documenting the protests.

During their detention, they were told that the crimes they were guilty of, documenting and spreading media of protests, were a far worse a crime than actually participating in the protest itself.

Fortunately, due to their American passports and support from the White House, they were treated fairly and made it home. Chinese and Tibetan activists, bloggers and journalists who have been arrested for similar acts have faced far worse treatment and sentences.

During last year's presidential elections, I was a member of a diverse team of software developers and open government activists who came together to build "Twitter Vote Report", a nation wide web 2.0-style election monitoring system that tied together google maps, wikis, and iPhones with human resources on the ground from watchdog groups and the media. Over 30,000 citizens reported from outside their polling places, providing a real time view and instant notice of any long lines, hanging chads and potentially voter fraud. The data captured that day was released freely to the Internet for analysis and research by academic institutions. The open-source code from this project, as well as a few others, has been utilized in India and Afghanistan, and we hope to see it become a standard tool in the fight against election fraud. It is important to remember that using technology to promote civic engagement and democratic participation is as important as its use for active dissent.

As you can tell, I am very enthusiastic and active participant in the use of new media tools for social good and in the fight against authoritarianism. However, the use of these tools also brings about the possibility of serious risk to the user, their friends, family and broader movement. As a friend of mine said, "You cannot twitter your way out of a bludgeoning by security goons". Mobile phones are unique, always broadcasting personal identifiers; changing SIM cards does nothing, phones are tracked easily tracked by their hardware IDs.

Laptop computers are often full of incriminating documents, web caches and email addresses. Digital viruses that deliver powerful espionage-ware such as GhostNet are common and becoming more powerful and more invisible every day—one slip and your entire email inbox can be copied by an adversary. Use of new media and social networks reveal one's "social graphs", buddy lists, friends & followers—in a free country, these provide benefit, amplifying your ability to communicate and connect. In an authoritarian state, these same tools can make clear loose connections between activists, which make the job of cracking down on dissent much easier and more efficient. It often takes an entire generation to rebuild when an activist network is decimated. The protests of 2007 and 2008 in Burma and Tibet were at level not seen since 1988 and 1989. That twenty year gap is no accident. Rather than just focus on the use of technology as a better megaphone, we need to consider how it can be used to safeguard and protect the identities and well-being of dissidents. The Tor Project is a successful case of technology that provides anonymity to web surfers and the ability to route around state-sponsored censorship.

While the free world is easily enamored of applications of new media tools within dictatorships and authoritarian states far way, our own federal, state and local law enforcement are often quite fearful and hostile towards their use within domestic movements. I raise this point not to say that we do not enjoy great freedoms in this democracy, but in order to make clear that tools which provide a more powerful platform for dissent are universally threatening to those in power. Tad Hirsch, creator of TXTMob, is the subject of a subpoena by the City of New York in connection with several active lawsuits against the City that allege police misconduct during the 2004 Republican National Convention. Elliot Madison, a 41 year old social worker, was been arrested in Pittsburgh on Sept. 24 and charged with hindering apprehension or prosecution, criminal use of a communication facility and possession of instruments of crime. The Pennsylvania State Police said he was found in a hotel room with computers and police scanners while using the social-networking site Twitter to spread information about police movements. Just this week it was announced that In-Q-Tel, the CIA's venture capital arm, has invested in a company whose technology is capable of powerful data mining from any information openly published on Twitter, Facebook and other social networking sites. In summary, measures taken to secure our homeland from violent terrorists often have similar justifications to those taken by authoritarian governments to squelch dissent and democracy.

We all must be mindful of these contradictory positions on the benefit of new media within our own democracy.

In summary, there are constructive steps that can be take today by policy makers, NGOs and technology developers. We need to support the development of a Global Technology Bill of Rights that extends freedoms of speech and the press to the tools needed to communicate using the Internet and mobile phones. Congress should develop policy and programs that recognize and fund new media technology as a fundamental component to the promotion of human rights, liberty and democracy. There also must be guidance and motivation for corporations, startups and venture capitalists who are building these technologies to consider their global impact on human lives, and not just on the bottom line or their stock price. I am all in support of entrepreneurs being rewarded for their risk, and am happy that tools such as Twitter can be used just as well to cover the daily lives of Ashton and Demi or break the news of Michael Jackson's death, as it can to broadcast updates live from the streets of Iran or spread the news of the execution of four Tibetan political prisoners this morning in China. I just hope that MBA students at Harvard and Stanford will consider the Humanity Quotient of their work while dreaming up the next big thing.

Finally, I would like to briefly emphasize the comments from Mary Joyce of DigiActive, who could not be here today, on the topic of embargoes. In the digital age, where a "good" is a string of code that can be delivered anywhere in the world with the click of a mouse, even today's smart sanctions are not smart enough. By preventing access to blogging platforms, social networks, and other types of new media, current embargo policies harm the very activists who are furthering our common goals of democracy promotion, while leaving authoritarian governments free to spread propaganda through a range of state-controlled media outlets.

Referenced web resources of note:

TXTMob: <http://en.wikipedia.org/wiki/TXTMob>

Alive in Baghdad: <http://aliveinbaghdad.org/>

TwitterVoteReport: <http://twittervotereport.com> Beijing Olympics Protest Coverage:  
<http://freetibet2008.tv>  
GhostNet: <http://en.wikipedia.org/wiki/GhostNet>  
Tor Project—anonymous web browsing—<http://torproject.org>

## **PREPARED STATEMENT OF EVGENY MOROZOV, YAHOO! FELLOW, GEORGETOWN UNIVERSITY, CONTRIBUTING EDITOR, FOREIGN POLICY**

I want to express my appreciation to the Members of the Helsinki Commission for holding a hearing on such an important subject today and for giving me the opportunity to share with you some thoughts drawn from my research into how authoritarian states are dealing with the challenges and opportunities presented by the digital age in general and new media in particular.

While I share much of the recent enthusiasm about the positive role that new media could play in opening up and democratizing authoritarian societies, I am increasingly concerned with both how well authoritarian governments have managed to adapt to the Internet threat and how poorly some digital activists, journalists, and even policy-makers understand the risks of trying to promote democracy via the Internet. Let me outline several of my most pressing concerns.

I. New media will power all political forces, not just the forces we like. Many of the recent Western funding and media development efforts have been aimed at creating “new digital public spaces”, on the assumption that these new digital spaces would enable the nascent actors of civil society in places like Egypt or China to flourish on blogs and social networks. While this does sound reasonable in theory, in practice we have to be prepared that groups that are often anti-democratic, both in their nature and rhetoric, would probably benefit most from the existence of such new spaces. In a sense, promoting these new digital spaces entails the same risks as promoting free elections: it’s quite possible we may not like who wins them. For example, research into the blogospheres in Egypt, Palestine, Russia suggests that Muslim Brotherhood, Hamas, and various groups of Russian nationalists and fascists have been one of the heaviest users of blogs and social networks (in part because they are often blocked from any access to traditional media, so for them these spaces are the only platforms). Blind support for promoting blogging and social networking may have a lot of very unpleasant unexpected consequences.

II. Authoritarian governments have developed extremely sophisticated strategies to control cyberspace. It is a mistake to believe that authoritarian governments wouldn’t be able to manipulate these new public spaces with their own propaganda or use them to their own advantage. Many authoritarian governments are already paying bloggers and Internet commentators to spin the political online discussions that they do not like. Strategies to build what I have dubbed “the spinternet” vary from country to country. The Russians outsource it to new media start-ups who then create ideological social networking/blogging sites that promote a pro-Kremlin ideology. The Chinese have created a decentralized and 280,000-people strong contingent of what is known as “50 cent party”—50 cent refers to how much they get paid for each comment they leave online—whereby its “blog” soldiers are tasked with identifying sensitive online discussions and trying to hijack the conversation in directions favorable to the government. The Nigerian government has been reported to be working on an “Anti-Blogging Project” that would fund hundreds of pro-government voices to counter the growing influence of the oppositional bloggers—and pay them in cyber-cafe vouchers. Even the Iranian clerics have been running Qom-based blogging workshops—particularly targeting women—to control much of the online discourse about religious issues (they obviously do not want any competing interpretation of Shia to take hold online).

III. Authoritarian governments are increasingly eager to build short-term alliances with digital groups that share their goals. One of the reasons why Russia has emerged as the most feared player in the field of cyberwarfare is because it always acts indirectly, usually by relying on numerous nimble underground gangs of cyber-criminals. Most of the time these gangs perfect the art of stealing credit card details of foreigners. However, when the geopolitical pressure so requires, they could be easily mobilized to assist the state (just think of the cyber-component to the recent conflicts Russia had with Estonia and Georgia, when the communication networks of both those states were crippled). Arguably, the fact that it's networks of cyber-criminals who plan and executive the attacks—perhaps, with barely concealed toleration and even tacit encouragement by the Kremlin—gives Moscow a different kind of power. Now, it can deny its direct involvement in the cyber-attacks (as it has done), while sending a clear message that anyone who wants to argue with it would have to be ready to deal with its cyber-gangs. Equally disturbing are recent movements by the governments to legitimize Internet censorship by involving fake institutions of civil society in the deliberation process. For example, on the suggestion of the speaker of the upper chamber of the Russian parliament, Kremlin may soon create a “Bloggers’ Chamber”—another one of those state-controlled fake representatives of the “civil society”—that would invite prominent Russian bloggers (but almost certainly bypassing those that disapprove of the Kremlin’s policies) to set their own standards of what can and cannot be discussed on Russian blogs. That’s just another example where the supposed ceding of state power would probably only reinforce the Kremlin’s control over the Russian Internet.

IV. Cyber attacks have become an important form of exerting indirect psychological pressure on civil society. Distributed denial-of-service (DDOS) attacks—whereby servers of a given Web site are overloaded with bogus requests to “serve” a page—don’t only make important content temporarily inaccessible, they also put a huge drain on staff and physical resources of an NGO or a newspaper. While the media tend to focus almost exclusively on cyber attacks against military and government targets—the overblown coverage of “cyberwars” in Estonia and Georgia have brought such dramatic terms as “cyber-Katrina” and “electronic Pearl Harbor” into public use—civil society organizations are hit the hardest. If left unchecked, DDOS attacks, which are increasingly cheap to organize and can be rented on the black market, may erase all the social capital that NGOs and even bloggers have cultivated online. The oft-quoted story of CYXYMU, a popular blogger from Georgia, is a case in point. A refugee from the earlier war in Abkhazia, CYXYMU emerged as one of the most visible and consistent critics of how both the Russian and Georgian governments handled last year’s war in South Ossetia. Blogging in Russian, he has cultivated a relatively large following in both countries, particularly among the users of LiveJournal, one of the most popular blogging platforms in post-Soviet cyberspace. However, in October 2008, somebody got angry at his writings, and his blog—also hosted by LiveJournal—fell victim to a massive wave of cyber attacks, so severe that millions of other LiveJournal blogs became inaccessible for more than an hour. We should recognize CYXYMU for what he is—a “digital refugee” and a victim of geopolitics playing out in cyberspace, where free speech is possible in theory, but increasingly unavailable in practice.

CYXYMU is not an isolated case. On the first anniversary of the monks’ uprising in Burma, a similar fate befell the three major Web sites of the Burmese exiled media—Irrawady, Mizzima, and the Democratic Voice of Burma. Administrators of the Web sites

speculated that the attacks were launched by the junta to limit expected demonstrations. Oppositional Web sites in Kazakhstan and Mauritania have recently experienced similar problems, quite possibly at the hands of their own governments or agents affiliated with them. Nonpolitical Web sites are becoming regular targets of cyber attacks as well: in February 2009, virtually all major gay and lesbian Web sites in Russia were unavailable for more than a week, as a result of a massive wave of denial-of-service attacks. In other words, that many anti-government discussions have moved online doesn't mean that these discussions would become any louder.

V. We do not fully understand how new media affects civic engagement. We shouldn't assume that establishing unfettered access to information is going to push people to learn the truth about human rights abuses/other crimes of the regime (and thus, make them more likely to become dissidents). Most likely, lifting the censorship lid would result in people using this opportunity to fill in other gaps in their info vacuum—those may have to do with religion, culture, socializing, and so forth. Political activism/active citizenship would probably only come last in this “pyramid of cyber-needs”. The creators of tools like Psiphon and Tor, which allow for anonymous access to banned resources, report that many users like these tools because it gives them access to downloading pornography, which is not as easy to do in tightly-controlled societies. In China, two-thirds of the respondents to one opinion poll agreed with the proposition that “It's possible to have real relationships purely online,” compared with one-fifth of Americans who felt the same. Just because a handful of young activists are turning to Twitter and Facebook to push for political change, we shouldn't automatically assume that thousands of others would follow. In fact, there is a growing risk that they would be sucked in into an endless cycle of infotainment, and their commitment to political life would be significantly eroded.

VI. The losses in online privacy may not be worth the gains in online mobilization. The emergence of new “digital spaces” where dissenting conversations can occur inevitably leads to the emergence of new ways to track those conversations. The proliferation of social networking has inadvertently made it easier to gather intelligence about whole networks of activists at very low costs. Even a tiny security flaw in the settings of one's Facebook profile may compromise the security of many others. While many established activists take the necessary precautions to remain undetected, it's the amateur, “spontaneous” activists who are at greatest risk. Selective intimidation of bloggers—coupled with a real (or perceived) ability to track online conversations—erodes the trust that aspiring activists place into “social media” and eventually makes them less likely to partake in protest movements. The old, “analogue” model of activism was arguably much safer: if one node of the network got identified/de-activated, there was little or no damage done to others, because they were much harder to trace in physical space. The new, “digital” model puts entire networks at risk, because getting access to an activist's inbox can put all of his interlocutors at risk. Moreover, by overlapping different “social graphs”—an Internet jargon for “one's connections on a social network”—it may be possible to reveal identities of people who have taken all precautions to remain anonymous. It's also important to remember that obtaining that password may not require any sophisticated knowledge of technology; as the prominent Egyptian blogger and activist Alaa Abd El Fattah once remarked to me “when torture is cheap, you are not as concerned with what they can do to you technologically”.

VII. New media development is an extremely complicated business that often has adverse unexpected consequences. Many of the latest attempts to create new “digital

public spheres” from abroad/with foreign funding might have adverse effects on their future health/sustainability. The very business of “new media development”—so eagerly embraced by Western governments and foundations—at this point looks very dubious (I am speaking as someone who has directed new media activities at a media development NGO funded by most big donors and as someone who now sits on a foundation board investing into new media). The injection of cash into foreign-based NGOs who are then expected to promote “social media” in a given authoritarian country usually means that they make smart, entrepreneurial new media whizzes of this country addicted to grant money; soon they become unwilling to work for free or don’t bother creating their own unprofitable projects. New media is usually a low-investment/high-reward business and the reason why we have so many interesting new media sites in the US or Western Europe is because it’s cheap to start, experiment, fail and move on to the next project. When you look at a grant-driven new media environment in a country like Belarus, what usually happens is that projects last for longer than they need to—they are not driven by business realities but rather by the bureaucracy of grant-reporting—and they usually commit the brightest minds who may otherwise be working on something else. In other words, the business of “new media development” suffers from all the classical pitfalls of economic development—and many more pitfalls of its own.

VIII. Current US government restrictions on the export of technology to sanctioned countries thwart the adoption of new technologies. I would also like to point out that the current sanctions against many authoritarian regimes—such as Cuba, Iran, North Korea and several others—make it significantly difficult for their ordinary citizens (as well as well-established activists and NGOs) to take advantage of all the opportunities that the Internet and social media offers. American technology companies face a fairly complicated process of obtaining and renewing licences and waivers to be able to export their technology to the sanctioned countries. These rules are not 100% clear and some tech companies decide not to take any risks and withdraw from these markets altogether. For example, some American hosting companies refuse to deal with customers from Zimbabwe or Belarus or Iran; this inevitable leads to implicit censorship, where activist groups—that are actually supported and recognized by the US government—have to justify their activities to Web administrators of these companies. What has not been widely discussed during the recent events in Tehran is that these protests succeeded, to a large extent, despite all the hurdles that the US government has imposed in terms of accessing these new media technologies.

Mr. Chairman, Mr. Co-Chairman, members of the Commission, thank you for giving me the opportunity to address you today.

## **PREPARED STATEMENT OF SHIYU ZHOU, DEPUTY DIRECTOR, GLOBAL INTERNET FREEDOM CONSORTIUM**

Mr. Chairman, Ranking Member, members of this Commission, ladies and gentlemen:

The Internet is a vast, fast, and inexpensive way to access information, to communicate, and to organize. It is perhaps the greatest hope for global information freedom and democratization, and it provides an important vehicle for the development of civil societies.

While authorities in closed societies can easily shut down newspapers, block TV channels, jam short-wave radios and ban books, control of the Internet is far more elusive and difficult to attain. But this is not for lack of effort. In the past decade, repressive governments around the world have invested heavily in censorship and surveillance of the Internet.

China is perhaps the best example of systematic control of the Internet. Tens of thousands of cyber police engage in monitoring and surveillance of Internet users, some of whom end up in prison for voicing their opinions online. China's "golden shield"—censorship technologies developed with the help of western corporations like Cisco—blocks many websites completely, and filter out topics deemed too politically sensitive by the ruling party.

China's model of Internet censorship is now being emulated elsewhere. The repressive governments such as that of Burma, Cuba, Iran, and now some Central Asian states of the former Soviet Union, are increasingly adopting technologies to stifle dissent, control information, and prevent citizens from communicating with the outside world. The Internet censorship firewalls have become the 21st century Berlin Wall that separates our world.

Yet amid the darkness of the Internet censorship in closed societies, a shred of light still remains. It is the Internet lifeline offered by the anti-censorship systems like that of the Global Internet Freedom Consortium—GIF for short, which has been providing millions in closed societies with free access to the Internet for years.

GIF consists of a small team of dedicated Chinese-American engineers, including myself, who were brought together by our practice of Falun Gong. Many of us were also among the students on Tiananmen Square during the 1989 Massacre, and we watched in the days and weeks that followed the massacre as the government began to rewrite history and distort the truth. We relived a similar experience in 1999, when the Chinese regime banned the Falun Gong spiritual practice and engaged in a campaign of misinformation and censorship to turn public opinion against Falun Gong, and to suppress news of the brutal persecution being carried out.

Through these events, we have personally experienced how frightening the state-controlled media can be—it confounds right with wrong, incites hatred, and institutionalizes ignorance. It is our belief that free flow of information is the most effective and powerful way to peacefully transform a closed society and promote human rights and civil liberties.

This conviction has driven us to spend many sleepless nights contending with the tens of thousands of Internet monitors and censors in China and around the world so that the citizens inside those repressed countries may safely communicate with each other and with the world. The men and women of GIF maintain operations out of our own pockets,

but we provide our products and services to the citizens of closed societies entirely free of charge.

We have developed a series of software programs—most notably FreeGate and UltraSurf—that provide users with encrypted connections to secure proxy servers around the world. We constantly switch the servers IP address at a rate of about 3,000 times per hour in the earlier time, now about 10,000 times per hour, so it makes the censors more difficult to block.

After years of hard work, our anti-censorship system has attained a global reach—it is used by people from almost every closed society in the world, and has been supporting the largest user base in the world's most censored countries like China, Iran, and Burma. Today approximately over 90% of anti-censorship traffic comes through our servers.

During the Saffron Revolution in Burma in late August 2007, we experienced a three-fold increase in average daily traffic from Burma. Many Burmese used our system to post photos and videos of the crackdown to the outside blogs and websites. The Burmese government had to entirely shut down the Internet to stop the outflow of information about the suppression.

Before the Beijing Olympics, when uprisings in Tibet led to thousands of arrests and large-scale human rights abuses, we saw our traffic from that region increase by over 400%.

Perhaps the best example of the role of GIF software was during the Iranian elections this past June, when our traffic from Iran increased by nearly 600%. On the Saturday of June 20, an estimated over 1 million Iranians used our system to visit previously censored websites such as Facebook, YouTube, Twitter, and Google. The Iranian users posted videos, photos, and messages about the bloody crackdown.

GIF systems have also been of benefit to US-based organizations such as Human Rights in China, Voice of America, and Radio Free Asia—and even companies like Google and Yahoo who self-censor, since we bring the uncensored version of their services into closed societies.

In fact, when the U.S. Internet companies such as Google, Yahoo, Microsoft are criticized for complying with the censorship demands of dictatorships, they often claim that they have few options but to do so. However, powerful anti-censorship systems make it effectively impossible for the regimes to demand censorship of those companies' in-country sites. This is because the more in-country sites are compromised by censorship demands, the more likely people in those countries will be to ignore them and to hook up to the uncensored overseas sites through anti-censorship systems.

The services GIF provides are invaluable, and the impact goes far beyond the Internet. When the people in closed societies gain a taste of freedom and are given a way to share information, they will no longer acquiesce to tyranny and injustice. Internet freedom has the potential of transforming the closed societies in a peaceful but powerful way that must not be underestimated.

Imagine what it would mean, for instance, if the Pope were able to conduct a web-based service with half a million house church Catholics in China. Imagine if the President of the United States could hold interactive town hall meetings with hundreds of thousands of Iranian students, or for Burmese, Syrians, Cubans, Tibetans, others to have full, free and real-time ability to communicate with each other and with supporters throughout the world. Imagine, if you will, how much safer the world could be, how much

better we could understand each other, and how quickly authoritarianism and repression would collapse when confronted with an engaged, educated, and free citizenry.

This may sound far-fetched, but consider this: for every dollar we spend on anti-censorship technologies, repressive governments must spend hundreds—perhaps thousands—of dollars to block us.

Congress is now considering a \$30m appropriation for Internet freedom that, if passed, could allow us to increase our current user capacity from 1.5 million people per day up to 50 million per day, and allow us to greatly enhance the rate at which our technology switches users' IP addresses. These developments would make it prohibitively expensive for any repressive government to counter our efforts.

The information warfare over the Internet has now boiled down to the battle of resources. We have the technology and the commitment. With a modest amount of resources, we will have the capacity, and together we will be able to tear down the 21st century Berlin Wall.

## **MATERIAL SUBMITTED FOR THE RECORD BY OLEG BREGA, FILMMAKER, JOURNALIST, CIVIL SOCIETY ACTIVIST FROM THE REPUBLIC OF MOLDOVA**

I'm Oleg Brega, 35 years old, a filmmaker and journalist from the Republic of Moldova. I represent civil society of this country, because I'm involved in several different NGOs, the most known of which, here and abroad, is the Hyde Park Association, a group of young people promoting freedom of expression, human rights in general.

7 years ago we organized a popular radio talk-show with the same name, which was closed down by the authorities.

After that we acted as an officially registered NGO, organizing weekly meetings in the central park of Chisinau, issuing a small newspaper with people's opinions. We have received grants from Norway and USA for supporting our activities.

But two years ago we decided to dissolve officially the organization because of the pressure from the authorities. It was a form of our protest against the permanent harassment, arrests, and illegal ceasing of the peaceful demonstrations, and interminable trial processes. In the same time, we stopped all our public activities on the streets, and we continued to be active only on the Internet, through the public blog Curaj.Net. There anybody could and still can express opinions, make announcements, report abuses.

In April 2009, I was employed as cameraman by a local private and independent television outlet, Jurnal TV, broadcasting only on the Internet.

I assisted at the vote counting on the Election Day and I also filmed the first protests against the results of the elections.

My brother, Ghenadie, another filmmaker, freelance journalist, former president of the Hyde Park, was one of the organizers of the public demonstrations on the next day after the elections. He, together with other young people invited everybody to come with candles at 6 PM on 6th of April in the central square of Chisinau, to show our disappointment and disagreement with the election results and against the way the election was conducted.

They used, in those available 6 hours, not only Twitter (some not at all, i.e. I made a Twitter account only after the so called Twitter Revolution) but all other available social networks and new media: Facebook, Netlog, especially Russian Odnoklassniki (my brother had there groups of thousands of subscribers, which he announced immediately about the intentions to protest), but the most important was the instant mobile messaging service. I send many SMSs and received during that day some SMSs from unknown persons, inviting me to the protest. Some were sent from the websites of the mobile companies, which some permit to send unlimited or others at least 20 messages per day for free. Also, the internet messaging as, Skype, MSN, Meebo were fully used. My list of friends on Yahoo Messenger, for example, has at least 500 addresses, and I used it to send in one minute short information with a link to the message about the demonstrations. It was spread instantly by my friends to other thousands of addresses.

These tools, together with many blogs, online forums, mailing lists and e-groups permitted to inform the most active people in Moldova about the action. This explains why a huge crowd was gathered on 6th of April in the center of the city. Most of the population couldn't accept that a political party (the communists), after 8 years of bad governing was able to take a half of the votes, to have again the majority in the Parliament.

But, probably, not only that initiative group, called “I’m anti-communist!”, was a real organizer. In the same day, after the closure of the peaceful demonstration, when the organizers invited people to go home and prepare for the next day’s meeting (initiated by the opposition parties), there were many provocations and violent actions. Nevertheless, the meeting ended before midnight, without damages, without arrested or injured people.

On the next day, on 7th of April, the organizers came late in the central square, with only megaphones and a small acoustic instillation. But, somebody else took control of the crowd, influence its behavior, and in a few hours, the Presidency and Parliament buildings, also some police cars, fire trucks, TV station’s car were destroyed, a lot of policemen, especially unprepared, inexperienced soldiers were injured in the street fighting, and it was almost impossible for the real organizers of peaceful protests (from the opposition parties) to stop the violence.

The authorities, police chiefs did nothing to stop violence, instead gave contradictory orders, provoked protesters, and, finally, after midnight, they ordered violent mass arrests. Hundreds of persons, even those who did not participated at protests were beaten. At least, three persons have died during that operation as a result of injuries.

In the following days, the Moldovan Government decided to close borders with Romania, to limit access of the foreign press, and to initiate in the state controlled media a campaign of accusation against the opposition and leaders of civil society.

Although demonstrations on 6–7 April didn’t change the results of elections, the behavior of the authorities made it impossible any collaboration within the Parliament between the Communist Party and the opposition parties. Communist MPs lacked one vote to elect a new president of the country, and, according to the electoral code, this triggered new parliamentary elections.

On July 29th, Moldova voted for a non communist majority, which formed a new governmental coalition, more democratic and pro-western, pro-Europe. It holds now most of the executive power in the state, and these days they are trying to elect a new, democratic president.

## **MATERIAL SUBMITTED FOR THE RECORD BY MARK BELINSKY AND EMILY JACOBI, CO-DIRECTORS, DIGITAL DEMOCRACY**

Commission members, we want to begin by thanking you for calling upon this briefing. We greatly admire the Helsinki Commission's tireless commitment to international diplomacy and universal human rights, and we commend your support for citizen movements using new media to challenge authoritarian regimes. As the use of these tools increases worldwide, it is critical for policy-makers to understand how they can be used to empower communication and collaboration among civil society activists.

### **THE PROBLEM**

Repressive regimes thrive on the distortion of truth. They rule through misinformation and fear. New media tools pose a challenge to this culture of fear, providing an opportunity for increased transparency. However deploying these tools in repressive environments brings significant hurdles:

1) New media technologies are often hardest to access within repressive regimes, where their use is restricted or censored.

2) New media technologies pose risks to users by potentially identifying them and their contacts as targets in places where dissent is criminalized.

3) Combined, these challenges can be life-threatening. When fewer people use social media, those who use it for political engagement are easier to track, trace, and punish.

Bloggers from Burma, Facebook users from Iran and Twitter users in Moldova have all been jailed for their use of new media in the past year. Social media, by making information more accessible, can lower the bar for participation, while increasing the risk of blowback to participants.

### **THE CASE OF BURMA**

In March 2007 we met "Stanley," a Burmese computer programmer living as a refugee in Thailand. In the mid-90s, he was targeted by the regime for his political affiliations and sentenced to seven years of hard labor. He witnessed many friends die before a harrowing escape to Thailand in 2005. After crossing the border, he founded an organization, the All Burma IT Student Union, dedicated to using Internet and Communications technologies to support democratic change inside the country, and develop the capacity of civil society. Based on his own experiences suffering from misinformation and human rights abuses from the Burmese regime, he has devoted his life to helping his people access information and tools while creating the critical technology infrastructure that community organizations for civil society to develop.

Stanley was one of nearly a hundred youth from Burma whom we interviewed for the Center for Peace Building International report *Overcoming Obstacles, Creating Opportunities*. Surveys with these youth revealed a correlation between internet access and self-identification as activists. In the interviews, the young people explained how internet access decreased the isolation of refugee life, inspiring hope by connecting them to the larger world. Explained Joseph Win, one of the young activists interviewed in the report:

“In my community we don’t know about human rights. We cannot get any information about human rights, the government controls all information. So that’s what I’m interested in.”

At the same time that we were observing the empowering potential of Internet access, we also worried about the risks. Many young people who were beginning to sign up for Facebook and other social networks travel back into Burma frequently, and didn’t understand how revealing personal information via social networks could endanger their safety. In further research, we’ve found that many Burmese civil society groups are aware that government might use new media for surveillance, but do not know the best ways to protect themselves from potential surveillance. These tools default on open access to information and make it difficult if not impossible to set different privacy settings.

In September 2007, both the power and danger of new media and Internet technologies came into sharp relief. Burmese citizens, led by Buddhist clergy, took to the streets in the largest protests in a generation. Despite less than 1% mobile phone and internet penetration at the time according to OpenNet Initiative, these tools were used to coordinate the protests and broadcast images of them internationally. Monks hid camera phones in their robes, and citizens took pictures from balconies and rooftops. Stanley, who was helping to disseminate this information later explained:

“During (this time), most of my time was spent on the Internet and mobiles in order to get real-time information from inside Burma to the international (community). Mobiles were used in taking images, movies and communication, but mostly used for reporting and networking among activists and politicians.”

The images and footage taken by Burmese citizens graced the covers of international newspapers and became reports on CNN, BBC, Al Jazeera and others, as people wondered how this was possible in a country where in protests just 20 years prior few photos had escaped the country and thousands were quickly beaten, jailed and even killed.

#### THE DANGER

On Sept. 27, 2007, nearly two weeks after the start of protests, the Burmese military forcefully responded to the peaceful protesters, attacking them with tear gas and then bullets, and raiding monasteries. The ongoing media coverage sparked international outrage. On Sept. 29, the military cut off all internet and mobile phone connections for five full days—a blackout on international coverage. During this time the military forces were able to quell remaining protesters, and jail still unknown numbers of dissidents. By the time limited internet access resumed, international attention had shifted.

The Burmese junta’s actions have set a frightening precedent for other authoritarian regimes. In June of this year, the Iranian government throttled mobile phone and internet access to crack down on citizens protesting for their votes. In countries where the government controls mobile phone and internet service providers, it is all too easy for them to shut down and otherwise manipulate information channels. Governments have also been savvy about tracking through new media sources to find and punish protesters. In the year following the 2007 protests, the Burmese military tracked down and imprisoned protesters using images and video, and the Iranian government has used Facebook profiles to identify—and punish—networks of dissent. In countries where torture is commonly used in interrogation of protesters, a Facebook “friends list” can provide a road map for authorities to find other people to target.

American corporations are also culpable. US corporations sell software to authoritarian regimes that allows them to monitor and censor information. In September 2005, Jerry Yang, co-founder and senior executive of Yahoo Inc., the global Internet giant, confirmed that his company gave Chinese authorities information later used to convict a Chinese journalist, Shi Tao, stating “To be doing business in China, or anywhere else in the world, we have to comply with local law.” A lack of legal infrastructure prevents US corporations from protecting new media users in repressive regimes. Site owners are culpable for content in foreign states, even when data is physically housed on US soil in data farms, and legal frameworks have not yet been fully established for US companies to protect end-users.

#### THE POTENTIAL

Despite these very real dangers, new media technologies represent great potential. Take the case of Stanley, whose All Burma IT Student Union is now teaching computer skills to dozens of Burmese youth a year, and who is developing open-source tools that allow for collaboration and dialogue of community groups from his country. Open-source tools have great potential because they can be worked on collaboratively with developers from around the world and have higher security standards because, as the name suggests, the code is open to the public. This democratic software development process has been embraced by the United States Chief Information Officer Vivek Kundra and emerging government websites that encourage increased transparency and accountability, such as Data.gov and endeavors being pursued by the New York State Senate. These examples can be heralded as models for democratizing societies.

In Zimbabwe, another repressive society, new media has been used to document elections and strengthen civil society groups. In March 2008, elections were held. The lead opposition party, the Movement for Democratic Change, used camera phones to document the posted voting results in different precincts. Compiling totals, this evidence helped them demonstrate their share of the vote, a move that led to runoff elections and the current power-sharing agreement between the opposition and Robert Mugabe’s Zanu-PF party. In October 2008, we spent time doing research in Zimbabwe, interviewing civil society groups in Harare about their use of new media technologies in their work. From journalists to student activists, they spoke of the way Internet tools and mobile phones were helping them better organize and coordinate their work. One young woman, who had miscarried a baby when attacked by police in a protest, was excited about the potential for new technologies as demonstrated by the Obama campaign, and their use of new media to mobilize volunteers. She is part of a vibrant civil society inside Zimbabwe that uses social networking and multi-media to share information and keep people motivated, despite the continuing outrage at Mugabe’s continued rule.

On security issues, there are also many positive developments. Tools now exist to help citizens circumvent government repression and censorship. In repressive regimes across the world ordinary citizens are learning how to use proxy servers to access censored information, VPN tunnels to share information while protecting their identities, and encryption techniques including chat and email that protect individuals right to privacy.

## THE SOLUTION/OUR RECOMMENDATIONS

New media tools foster the dialogue and collaboration that are critical to engaged, empowered communities. How can US policy support this?

Support should be given to help community groups assess their needs and apply new media strategically to meet their goals. This support should not only come through official government channels, but through civil society actors across national boundaries. In Ambassador John McDonald and Louise Diamond's landmark book *Multi-Track Diplomacy*, they outline nine tracks of diplomacy: conflict resolution professionals, business, private citizens, media, religion, activism, education and philanthropy. Each track works in concert with the others, and all affect international diplomacy.

When considering policy that affects new media use in repressive societies, we urge US lawmakers to keep in mind:

1) Security: Understanding security and safety risks is critical to the successful application of new media under authoritarian regimes.

2) Local partnerships: When new media tools are built with local partners from repressive societies, they can incorporate local security concerns and address the cultural context, while developing the skills of local partners.

3) Grassroots media and technology trainings: Media literacy needs to be coupled with powerful media stories to develop a thoughtful civil society. Technology serves as the infrastructure to this and needs to be supported. emerging tools and solutions through trainings that are context specific. Encourage on-going skill and

4) Emphasis on education, communication and civic participation: Knowledge is power, and new media tools that educate, inform and motivate civil society are those that achieve the greatest impact.

In closing, it is critically important for decision-makers today to understand the ways in which new technologies are shifting the social, political and economic landscapes. This understanding can support and embolden projects which use technology and new media to foster education, communication and participation. We would like to end with the words of U Pinya Zawta of the All Burma Monks Alliance:

“ In Burma, the military controls all communications technology. But technology is very important to change. The Burmese military is trying to hide human rights abuses inside (the country). To show human rights abuses we need technology. People who are doing bad deeds need to be afraid.”

**MATERIAL SUBMITTED FOR THE RECORD BY MARY JOYCE,  
ANDREAS JUNGHERR, AND DANIEL SCHULTZ, WORKING  
GROUP ON SANCTION REFORM FOR THE DIGITAL AGE  
[DigiActive.org]**

Chairmen Cardin and Hastings, and Members of the Commission:

Thank you for granting us the opportunity to present written testimony on the role of new media in authoritarian regimes. Mr. Jungherr, Mr. Schultz, and I are representatives of DigiActive, an online organization that studies and promotes the use of digital technology by grassroots activists around the world. In our testimony I will relate several cases of digital activists living under authoritarian regimes whose pro-democracy activities are being thwarted. I will then identify the surprising source of this persecution, and offer a solution.

**A WAVE OF ATTACKS ON THE WORLD'S DIGITAL ACTIVISTS**

In the winter and spring of this year, a wave of attacks on digital activists began. In Zimbabwe, the web site of one the nation's strongest pro-democracy groups, Kubatana, was threatened with being shut down. In Belarus, another pro-democracy web site, this one representing the Belarussian American Association, received the same threat. In February bloggers in Iran received a similar notice that their blogs would be suspended, this in spite of research by the Harvard Berkman Center for Internet and Society that the Iranian blogosphere is a vibrant arena for both supporters and opponents of the current regime. In Sudan, aid workers are unable to download Google Earth and its "Crisis in Darfur" map, which would give them important information on sites of violence. In April users in Syria were temporarily blocked from using the social network LinkedIn, though social networks have played an important role in organizing grassroots citizen movements in countries from Egypt and Morocco to Colombia.

- Perpetrated by United States' Embargo Policies

Who was behind this wave of attacks? Was it President Mugabe? President Lukashenko? President Assad? No. The perpetrator of these attacks on pro-democracy activists was none other than the United States government and American companies adhering to its embargo regimes.

The United States has several embargo regimes related both to particular products (such as encryption software) and to individuals. These sanctions were designed to protect US interests while limiting the effect of these measures to our nation's enemies. Yet in the digital age, where a "good" is a string of code that can be delivered anywhere in the world with the click of a mouse, even today's smart sanctions are not smart enough. By preventing access to blogging platforms, social networks, and other types of new media, current embargo policies harm the very activists who are furthering our common goals of democracy promotion, while leaving authoritarian governments free to spread propaganda through a range of state-controlled media outlets.

- With American Firms Caught in an Untenable Position

These embargo policies leave American firms in a difficult position. Overwhelmed by a mass of overlapping sanctions, many take the most conservative position and simply cut off all clients in targeted countries, even though sanctions target only a few individuals. This was the policy of the Utah-based company Bluehost, which was responsible for cut-

ting off users in Zimbabwe, Belarus, and Iran earlier this year. Especially in light of potential fines, Bluehost decided to play it safe by cutting off all users in embargoed countries, rather than constantly cross-check their users against Specially Designated Nationals (SDN) lists.

Though activists may be frustrated with this kind of corporate decision-making, it is consistent with the firm's role as a profit-making entity. American companies may choose to promote ethical activity and protect activists in foreign nations, but this is hardly their purpose. When protecting activists means potentially running afoul of the US government, it is not surprising that many firms choose to cut off activists to protect shareholder interests.

#### NEW EMBARGO POLICIES FOR THE DIGITAL AGE

In light of these private-sector realities, responsibility for protecting foreign democracy activists falls to the US government. DigiActive's Working Group on Sanction Reform for the Digital Age recommends the following steps in order to bring about this reform:

1. **Creation of a Single Body of Software Regulations:** Members of the government bodies responsible for promulgating sanctions should conduct a thorough review of all regulations and legislation related to embargoes on software including, but not limited to, the Commerce Department's Export Administration Regulations and the sanctions programs maintained by the Treasury Department's Office of Foreign Assets Control. This review would result in the creation of a single volume of software policies which, at a minimum, will make it easier for US firms to abide by current rules and, by clarifying their responsibilities, would allow them to follow the letter of the law rather than taking the unnecessarily conservative positions they are currently applying to avoid the risk of transgressing unclear embargo regulations.

2. **Stakeholder Review of Software Regulations:** Once this single body of regulation is created, stakeholders should be invited to comment and suggest modifications to the existing rules. This stakeholder group should include, but not be limited to, representatives of the agencies responsible for promulgating and enforcing the sanctions, representatives of American firms who must abide by the sanctions, and experts in digital activism and democracy promotion.

3. **Promulgation of New Regulations:** Based on this stakeholder review, DigiActive suggests that a new set of sanctions be promulgated that recognize 1) that software embargoes function quite differently than embargoes on physical goods 2) that any software embargo is highly susceptible to failure because of the ease in circumventing online blocks to digital goods and 3) that access to new media tools is a great benefit to democracy activists, who lack other means of organization and message dissemination, while being of little use to authoritarian regimes, who have entire state apparatuses at their disposal.

We at DigiActive have great faith in the Commission on Security and Cooperation in Europe and in the United States government to reform the current sanction system and offer our continuing assistance during this process.

## **MATERIAL SUBMITTED FOR THE RECORD BY PATRICK MEIER,<sup>1</sup> DIRECTOR OF CRISIS MAPPING AND PARTNERSHIPS, USHAHIDI**

The information revolution, like any revolution, has the potential to change the balance of power between the have's and have not's. The question is: Does the information revolution empower the coercive control of repressive regimes at the expense of nonviolent resistance movements, or vice versa? Does the change in the means of, and access to, information significantly threaten authoritarian control?

We ask these questions because scholars and policymakers recognize that the “techniques associated with strategic nonviolent social movements are greatly enhanced by access to modern information communication technologies, such as mobile telephony, short message service (SMS), email and the World Wide Web, among others.”<sup>2</sup>

This explains *raison d'être* of Ushahidi<sup>3</sup> which was referenced several times during the Congressional Briefing on October 22nd.<sup>4</sup> Given that some of the comments made about Ushahidi were rushed due to time constraints, we wish to take this opportunity afforded to us by the Helsinki Commission to provide additional context on Ushahidi.

### WHAT IS USHAHIDI?

Meaning “witness” or “testimony” in Swahili, Ushahidi is a free and open source platform that combines Twitter, SMS, smart phone apps, email and dynamic maps such as Google Maps to crowdsource crisis information. This includes information on human rights violations and election fraud violence perpetrated by authoritarian regimes. The aim of Ushahidi is thus to document information that would otherwise go unreported. Since information is power, Ushahidi believes that a “crowdsourcing” approach has the potential to shift the balance of power in favor of greater transparency and accountability with respect to human rights and democratic freedoms.

Ushahidi was launched in January 2008 to document the post election violence in Kenya. Various partners have since deployed Ushahidi to document human rights violations and/or election irregularities in the Democratic Republic of the Congo (DRC), Gaza, Lebanon, Mexico, Afghanistan and Mozambique. A number of new partners have already signaled their intention to use Ushahidi in 2010 to document repression in several important countries under authoritarian rule. In addition, major humanitarian organizations like the United Nations and global media groups are partnering with Ushahidi to leverage the crowdsourcing of crisis information.

Finally, Ushahidi has received a number of prestigious awards and also important media coverage from the BBC, Reuters, The Economist, Forbes and several other respected sources. This is an important way to get the word out on Ushahidi so that would-be users are aware that the tool is freely available for them to download and use at any time.

---

<sup>1</sup>This testimony is submitted on behalf of the entire Ushahidi Team. Contact Email: Patrick@Ushahidi.com |Phone: 617.440.4442 |Twitter: @Ushahidi

<sup>2</sup>Cited in Meier, Patrick (2008). “The Role of New Media and Digital Technology in Popular Resistance against Authoritarian Regimes.” (PhD Dissertation Proposal, The Fletcher School, Tufts University). Available at: <http://www.iRevolution.net>

<sup>3</sup>Ushahidi: Crowdsourcing Crisis Information. Available at: <http://www.Ushahidi.com>

<sup>4</sup>See in particular comments made by panelists Nathan Freitas and Chris Spence.

## REFERENCE TO USHAHIDI AT BRIEFING

Some of the comments made by panelists at the Congressional Briefing on October 22, 2009 reveal a number of misconceptions about Ushahidi. This section of the testimony is an effort to redress these misconceptions.

Ushahidi, the tool, is deployed by other organizations interested in citizen-based monitoring. This means that Ushahidi, the organization, does not take the lead in implementing the platform around the world. This is done by other organizations such as human rights groups and local nongovernmental organizations (NGOs). Whether these groups choose to completely open the platform to the public (open crowdsourcing) or not (bounded crowdsourcing) is always their decision.

This is important to note since one recurring misconception of Ushahidi is that the tool is always used for open crowdsourcing. Not so. The platform has been used by organizations with known and trusted networks to “crowdsource” crisis information. In any case, the purpose of the tool is to collect and aggregate both verified and non-verified information. Indeed, as panelist Nathan Freitas noted in his comments at the Congressional Briefing, Ushahidi is “akin to a blog system, but for mapping crisis, and what’s unique about it is it allows you to capture unverified and verified information.”

But what actually is the difference between these two types of information in the first place? In general, unverified information simply means information reported by “unknown sources” whereas verified tends to be associated with known sources of reporting, such as official election monitors.

The first and most important point to understand is that both approaches to information collection are compatible and complementary. Official election monitors, like professional journalists, cannot be everywhere at the same time. The “crowd” in crowdsourcing, on the other hand, has a comparative advantage in this respect.

The crowd has many more eyes and ears than any official monitoring network ever will. So discounting any and all information originating from the crowd is hard to justify. One would have to entirely dismiss the added value of all the Tweets, photos and YouTube footage generated by the “crowd” during the post-election violence in Iran, for example.

This in no way implies that information verification is not important. Indeed, some groups that deploy Ushahidi decide to limit the information collection to known entities only. In addition, Ushahidi and partners are developing a platform called Swift River to verify crowdsourced information in near real-time.<sup>5</sup> That said, the purpose of the Ushahidi platform is to collect as much information as possible.

In other words, the purpose of Ushahidi is not replicate what other groups already do very well, such as official and statistically driven election monitoring. That said, the data generated by Ushahidi can nevertheless serve as corroborating evidence for the official data collected. Unfortunately, because of some misconceptions about Ushahidi, many experts overlook this.

Contrary to remarks made in the Briefing, users of Ushahidi to date do not seek to “reach certain thresholds” in order to make statistical statements about certain trends in human rights violations or election irregularities. That is not, and never was, the stated

---

<sup>5</sup> For more information on Swift River, please see: <http://irevolution.wordpress.com/2009/09/12/accurate-crowdsourcing-hr>

purpose of Ushahidi. Nor do groups deploying Ushahidi purport to be the only source of information for human rights or election monitoring. Like any serious research, a mixed methods approach drawing on a diversified set of sources is often the most prudent way forward. Only then is the process for rigorous data triangulation a legitimate possibility.

In sum, crowdsourced data can be an important repository for triangulation. The more crowdsourced information we have, the more self-triangulation is possible and the more this data can be used as a control mechanism for officially collected information. Yes, there are issues around verification of data and an Ushahidi powered map may not be random enough for statistical accuracy but, as Ushahidi co-founder Ory Okolloh notes, “the data can point to areas/issues that need further investigation, especially in real-time.”

Another relevant point worth noting is that many times official groups, whether for election monitoring or otherwise, often get shut down or deported. When these groups are no longer able to operate, citizens are often the only actors left and able to document human right abuses and election violence. Without official systems in place to report such incidences, what is really happening may go completely unreported. Ushahidi seeks to fill this gap, one that is all too often common in countries under authoritarian rule.

Take the case of the election violence in Kenya. There were thousands of official election monitors in country but when it came to sharing data on polling observations, these official actors (the EU and IRI) reneged on sharing their data because it was considered too “political”. IRI eventually released their data but some 8 months later even though they were supposed to act as the filter—the verifier of election data.

As Ushahidi’s Ory Okolloh states, “At a time when some corroboration could have prevented bloodshed, the ‘professionals’ were nowhere to be seen, so if we are talking about verification, legitimacy, and so on . . . lets start there.”

One more misconception revealed during the Congressional Briefing is that crisis mapping and crowdsourcing are one and the same. Crowdsourcing is a (relatively new) methodology for information collection. This information can then be mapped using various crisis mapping platforms and data visualization techniques. It is important not to confuse the two.

## CONCLUSION

To conclude, Ushahidi would like to submit for the record that the different approaches that exist for human rights and election monitoring are complementary and not incompatible. We need diverse methods and platforms in order to document, understand and respond to complex dynamics. Ushahidi, for its part, represents only one of many different possible approaches that can add transparency and accountability in countries under authoritarian rule.

## **MATERIAL SUBMITTED FOR THE RECORD BY MERICI VINTON**

Thank you to the Helsinki Commission for inviting me to speak today. It is truly an honor to be able to speak on such a prescient topic about how new media tools can help foster civic participation and strengthen the political process. Investing in new media is an investment in the relationship between government and citizens, political candidates and citizens, but most importantly, in citizens and citizens.

I wanted to share a bit of my background, as it provides the lens through which I will address the various issues facing us. I recently completed a fellowship with the Sunlight Foundation, where I assisted with the launch of two online advocacy campaigns. I joined the Obama campaign in the spring of 2008, first as a field organizer and then later I moved to the New Media team. I was the North Carolina Director of New Media for the general election and oversaw a team that used video, text messaging, blogging, facebook and MySpace (and countless other social networking sites), email and the my.barackobama.com organizing site to engage supporters and push them to action. With the exception of my.barackobama.com, none of these tools are new. Nor are they especially special. What is unique was how the campaign used the tools. I apologize if you have heard the following information about the Obama campaign; I include them because I have learned that how we used new media is still new to the vast majority of people. And many of these concepts are exportable.

When Senator Barack Obama decided to run for President, he wanted to run a campaign that would leave the political process better off, even if he lost. That decision set the tone for a campaign that was open to new ways of organizing, new technologies and new ways of communicating its message to the country. The campaign motto for staff and volunteers was “Respect. Empower. Include.” This motto and campaign ethos spoke to many—the campaign included over six million volunteers, five million individual donors and five thousand staffers spread out over all 50 states. When we said, “this campaign is about you,” we meant it—and people truly felt as though their efforts, however large or small, were making a difference. Having a presence in all 50 states was important, as we wanted to be able to engage individuals nationwide.

The campaign was a blend of national and local messages—and two-way communications. What set our campaign apart was that we listened. We told your story. We told Obama’s story. We let you tell your neighbors why Obama’s policies are going to have a positive impact in your neighborhood (and probably made a youtube video of it). The campaign structure was designed to have the various teams share the same message, just tailored for their appropriate outlets. If the message of the week was why Barack Obama’s economic policy is good for your community, the field team would organize economic house parties, the communications team ensured that this message had local surrogates on the nightly news and the new media team was everywhere else. We came to you and lived where you lived—social networks, your mobile phone (if you opted-in to campaign text messages), email and even video game advertising. We wanted to reach people directly to let them know there was room for them on our campaign. This allowed the campaign to go around the traditional media to bring its message to the people. On November 3, 2008, the new media team had uploaded 1792 videos totaling 18.5 million views. My comparison, John McCain’s team uploaded 329 videos with just over 2 million views.

The website behind the campaign’s online organizing might is my.barackobama.com, or mybo. [It is interesting to note that several architects behind mybo were members of Governor Howard Dean’s 2004 Presidential campaign. His campaign demonstrated that

people were ready—even hungry—to use the internet to self-organize via meetup.com] Mybo was a self-contained social network that allowed users to online phone bank, organize events, blog, fundraise and create affinity groups that served as listservs for like-minded individuals (for example: North Carolina Women for Obama or soccer players for Obama).

At the end of the campaign, over 2 million mybo profiles had been created, 200,000 offline events were planned and about 400,000 blog posts were written. The campaign revolutionized online fundraising, bringing in over \$500 million and approximately 90% of total funds raised.

Obama's election changed citizens' expectations of government—the campaign's supporters expected a more transparent government, while technologists expected a digital transformation with regards to government websites and innovation. President Obama's first memorandum to Federal employees outlined three principles of open government—government should be transparent, participatory and collaborative. And much of this change is internet-driven.

This is key—following the campaign, people now expect this from government. The campaign changed behavior and expectations of government. This is by no means a new concept, but hits at the core of ways the Helsinki Commission can foster change.

Government communications have taken a dramatic shift. Instead of relying on traditional media sources to spread news, government agencies and departments have taken to the Internet to directly engage citizens. It's not uncommon to see Cabinet level officials speak into a flip cam en route to a meeting. Suddenly government managers are training their employees on ways to use the Internet to engage citizens. Cabinet Officials and Departments have started popping up on social networking sites—you can be among the 35,000+ fans of NATO Secretary General Anders Fogh Rasmussen on facebook.com or follow the Department of Justice (@TheJusticeDept) on twitter. Don't mistake this for transparency, but rather these are attempts at making government more engaging and accessible.

Transparency efforts have increased dramatically and suddenly data is, well, kind of exciting. Organizations like the Sunlight Foundation argue that government data should be online and accessible for everyone. Ellen Miller and Michael Klein of the Sunlight Foundation write, "More transparency in politics will enable a healthy dynamic of rising public attention and engagement in demanding more accountability from government. Improved transparency is not a threat to public trust; it is the very basis for restoring that trust." By shining some "sunlight" on campaign donations or lobbyists, we can begin to build trust.

Now what to do what that data . . . Government holds data on everything from environmental quality to food safety to infrastructure spending. To be brief, if government releases data in machine-readable formats, developers can take that information and make it interesting to non-geeks. An example is Washington, DC's Apps for Democracy contest—they launched an initiative that took city data and opened it up to developers to see who could come up with the most innovative way to repackage this data and turn it into a tool. Some examples include overlaying bus transportation times on a smart phone based mapping program or databases that make government data easy to search for researchers and/or students.

I tell this story because, while it begins with a Presidential candidate, it only succeeds because of the efforts of millions of individuals. “New Media” does not challenge authoritarian regimes, people do.

The Helsinki Commission could find and support programs that train individuals in new media tools. At a new media forum in Tbilisi, Georgia, I worked with journalists and students on how to use new media tools to help foster a free press. Common problems cited by the conference attendees were lack of an independent press and little government transparency. Together we brainstormed to find ideas that would promote journalistic integrity and some easy ways to hold their government accountable—all ideas used free new media tools to help spread their message.

The Helsinki Commission has a strong commitment to building and strengthening democracy—by supporting programs that foster nascent civic participation, the Commission would be building the early foundations of democratic participation. From a technology perspective, the Commission could find and invest in in-country technologies that build community.

Based on this information, I recommend that the Helsinki Commission:

1. Invest in new media channels to better enable open and transparent dialogue between citizens and the state and between citizens themselves
2. Seek opportunities to work with existing new media channels and online communities to build on strong civic foundations to generate dialogue, collaboration and action within civic society
3. Provide a range of clear and transparent support and tools to enable people to better engage online, such as best practice guidance and web tools
4. Support individuals and organizations developing new websites, tools and techniques for engaging online, potentially drawing on initiatives such as Washington, DC’s Apps for Democracy











This is an official publication of the **Commission on Security and Cooperation in Europe**.



This publication is intended to document developments and trends in participating States of the Organization for Security and Cooperation in Europe (OSCE).



All Commission publications may be freely reproduced, in any form, with appropriate credit. The Commission encourages the widest possible dissemination of its publications.



**<http://www.csce.gov>**

The Commission's Web site provides access to the latest press releases and reports, as well as hearings and briefings. Using the Commission's electronic subscription service, readers are able to receive press releases, articles, and other materials by topic or countries of particular interest.

Please subscribe today.