Testimony
Ivan Sigal
Executive Director, Global Voices

at the hearing:
"The Promises We Keep Online: Internet Freedom in the OSCE Region"
Commission on Security & Cooperation in Europe, United States Helsinki Commission
July 15, 2011

Chairman Smith, Co-Chairman Cardin, and Commission members, thank you for the opportunity to address the Commission, and the topic of online freedom of expression in OSCE countries. I am Ivan Sigal, Executive Director of Global Voices, a nonprofit organization and community of bloggers, writers, and translators from around the world who analyze and amplify the most interesting conversations appearing in citizen media for global audiences.[1] Global Voices has a team of writers who cover issues of citizen media in Eastern Europe and the former Soviet Union.[2] They are also contributors to and authors of several recent research documents that focus on online rights and freedom of expression in countries of the former Soviet Union, and examine the tactics that governments use to suppress online speech.[3] Additionally, I lived and worked in the former Soviet Union from 1996 to 2004, primarily working with local media outlets on journalism and program production and training, media law and regulation, and media sector association building, with the media development organization Internews. My testimony is informed both by the work of the Global Voices community, and my own experiences.

While I am drawing upon work of the Global Voices community, the conclusions, analysis, and recommendations are mine alone: Global Voices community members hold a diverse range of viewpoints about the U.S. government's foreign policy, international organizations, and policies of other governments including their own.

The Global Voices mission reads in part, as follows:

> *We believe in free speech: in protecting the right to speak — and the right to listen. We believe in universal access to the tools of speech. To that end, we seek to enable everyone who wants to speak to have the means to speak — and everyone who wants to hear that speech, the means to listen to it. Thanks to new tools, speech need no longer be controlled by those who own the means of publishing and distribution, or*

[1] http://globalvoicesonline.org/.
[2] http://globalvoicesonline.org/-/special/runet-echo/, http://globalvoicesonline.org/-/world/eastern-central-europe/, http://globalvoicesonline.org/-/world/central-asia-caucasus/.
[3] "Freedom on the Net 2011: Russia," Freedom House, http://www.freedomhouse.org/images/File/FotN/Russia2011.pdf; Rebekah Heacock, "Second- and Third-Generation Controls Rise in Russian Cyberspace," OpenNet Initiative, April 7, 2011, http://opennet.net/blog/2011/04/second-and-third-generation-controls-rise-russian-cyberspace.

> *by governments that would restrict thought and communication. Now, anyone can wield the power of the press. Everyone can tell their stories to the world.*[4]

Global Voices seeks to listen to and amplify the voices of many people online, without specific advocacy positions on given issues. Instead, we support basic principles for speech and access that encourage civic participation. These concepts are in line with OSCE Charter commitments, as well as with Article XIX of the Universal Declaration of Human Rights.

To that end, ongoing restrictions and suppression of the tools of online speech in the OSCE region, the harassment, arrest, and imprisonment of individuals for exercising speech rights that are protected under OSCE and United Nations obligations, are a matter of concern, and a subject of our website's coverage.

While attacks on mass media in the OSCE region have occurred for years, and continue, with this document I am focusing mostly on attacks on individuals, citizen media communities, and social media networks. These targets have fewer resources, less experience, and face a different kind of risk than traditional mass media, which have institutional capacity, capital, and organizational standing, which, while making them targets, also offers them relatively robust protection.

Recent events have once again highlighted the disregard demonstrated by several OSCE member states seem to have for the protection of freedom of speech obligations expressed in numerous OSCE documents.[5] Specifically, we have seen restrictions and attacks on access to online platforms and social media networks, in response to protesters' use of those tools to organize. Prominent recent examples include Russia, Kazakhstan, Belarus, and Turkmenistan.

Protesters in Belarus, for instance, in June and July 2011 organized, documented, and amplified protests using social media platforms such as vKontakte. The membership in these vKontake groups numbered in the thousands with at least one group with nearly 214,000 members.[6] The size of these groups intimated the possibility of mass protests in Belarus, in rallies initially set for June 22, 2011.

[4] http://globalvoicesonline.org/about/gv-manifesto/.

[5] The OSCE has commissioned an extensive report regarding the legal and regulatory environments of OSCE member states by Yaman Akdeniz titled "Freedom of Expression on the Internet" (http://www.osce.org/fom/80723) that covers legal and regulatory practices of OSCE member states in relation to the following documents: Final Act of the Conference on Security and Cooperation in Europe, Helsinki, 1 August 1975. http://www.osce.org/documents/mcs/1975/08/4044_en.pdf. Budapest Summit Declaration, December 21, 1994. http://www.osce.org/mc/39554. Lisbon Summit Document, December 3, 1996. Official text at http://www.osce.org/mc/5869. Charter for European Security, adopted at the OSCE Istanbul Summit, November 1999. http://www.osce.org/documents/mcs/1999/11/4050_en.pdf. OSCE PC.DEC/633 on Promoting Tolerance and Media Freedom on the Internet, endorsed by MC.DEC/12/04 at the OSCE Ministerial Council in Sofia, 7 December 2004. http://www.osce.org/mc/23133.

[6] Alexey Sidorenko, " Belarus: Police Crack Down on Minsk Protest," June 24, 2011, Global Voices Online, http://globalvoicesonline.org/2011/06/24/belarus-police-crack-down-on-minsk-protest/.

The response of the Belarus government has been a creative mix of hacking and distributed denial of service (DDoS) attacks on vKontake groups, disinformation campaigns via videos on YouTube and Twitter, and intermittent blocking or slowing of access speeds to popular the social network LiveJournal.[7] Belarus authorities also went online, seeking to dissuade group members from participating. The Belarus Ministry of the Interior and the Minsk Police Department both launched Twitter accounts (@mvd_by, @GUVD_Minsk), which they used to discourage people from attending rallies and warning them of potential punishments should they appear at protests.[8]

This kind of multi-layered response by governments seeking to suppress or discredit online speech is increasingly becoming the norm in several OSCE member states, particularly in the former Soviet Union. While Turkmenistan and Uzbekistan practice extensive filtering, other countries such as Kazakhstan, Russia, Belarus, and Azerbaijan implement a range of responses that together serve to restrict online access to information, participation, and content creation, and monitor and surveil online communities.[9]

This mix of tactics of suppression and repression goes back at least 10 years. A combination of filtering and hacking of websites, physical threats and intimidation, propaganda and defamation, burdensome legal and regulatory environments, market manipulation, and the use of tertiary legal controls such as tax inspections worked to threaten an earlier generation of online content providers.

It is no secret that many governments in the FSU have gained their legitimacy through questionable means. Rigged elections, heavily biased and government-controlled media, dependent and corrupt judiciaries, opaque and vague laws and regulations, arbitrary implementation of law, and extralegal responses to political opponents including violence and killing are all too common. This has been true for some countries in the region since the fall of the Soviet Union, and has given governments a sense of impunity in regard to their behaviors.

Filtering and hacking of Internet content in the region now has a long history. Targeting of individual websites, online publications, or individual writers through a range of online and offline tactics is also not a new story. The concern is that as internet access grows across the FSU, governments will step up their restrictions, targeting not just relatively elite communities of writers and opposition politicians, but citizens writing and sharing

[7] Alexey Sidorenko, "Belarus: Independence Day Clapping Protest (Video). Global Voices Online, July 6, 2011, http://globalvoicesonline.org/2011/07/06/belarus-independence-day-clapping-protest/.

[8] Sidorenko, " Belarus: Police Crack Down on Minsk Protest." It has been reported that people trying to connect to Vkontakte have been redirected by Belarusian Internet service provider BelTelecom to websites containing malware. From early May to early June, at least seven websites were closed at the behest of the police, which was given new prerogatives under a law adopted on 1 March. The journalists who continue to be held in prison after covering protests are mostly freelancers or reporters working for news websites that the government does not register as news media (source: Reporters Without Borders, personal communication, July 14, 2011).

[9] OpenNet Initiative, "Access Denied: Commonwealth of Independent States profile," accessed July 14, 2011, http://opennet.net/research/regions/cis.

multimedia content on a range of user-generated platforms.

While tactics may change, the overall strategy of mixing the tools of repression to achieve various ends remains in place. The ultimate goal of this kind of harassing activity seems to be to systematically suppress speech and media content that questions the legitimacy of those in power, and particularly those who question how power and wealth are gained and distributed. It is notable, as well, that some of these practices are not restricted to non-democratic regimes. Recent mass media laws in Hungary also treat websites as mass media, for instance, and Italy's intermediary liability laws also function to suppress speech.[10]

The tactics employed to suppress speech are varied, and explained elsewhere in considerable detail.[11] A short list of common tactics:

Legal and regulatory controls

- Media licensing and registration regulations which treat websites as mass media, in Russia, Belarus, Kazakhstan, and most recently, Hungary and online forums in Russia, which targets social media networking sites
- Legal access to data tracking online behavior of users and data retention requirements based in security laws such as Russia's SORM-II regulations and equivalents in Kazakhstan, Uzbekistan, Ukraine, and Belarus
- Legal filtering and blocking of websites and webpages
- Intermediary liability requirements for content on social networking, search, and user-generated content websites
- Improper use of laws that restrict "bad" speech - hate, pornography, support for "terror", sometimes used to justify Internet filtering[12]
- Use of intellectual property regulations to restrict access to an entire website or type of website
- Lack of due process for protesting blocked or filtered content, lack of transparency about reasons for filtering, and lack of clarity regarding who is blocked/filtered, and at what level
- Imprecise language within law that leads to overly broad application of restrictions, for instance against "inappropriate" content (Uzbekistan) or threats to "public order" (Kazakhstan) and lead to self-censorship; lack of recourse or appeals processes

[10] "An Open Letter from the Hungarian Civil Liberties Union (HCLU) to the European Commissioner, Neelie Kroes, regarding the Proposed Amendments to the Media Law," One Million for Freedom of Press in Hungary, March 8, 2011, http://freepress.blog.hu/2011/03/08/an_open_letter_from_the_hungarian_civil_liberties_union_hclu_to_the_european_commissioner_neelie_kro.

[11] *Access Controlled, The Shaping of Power, Rights, and Rule in Cyberspace,*
Edited by Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski and Jonathan Zittrain, April 2010, MIT Press, Cambridge, MA.

[12] In June 2011, the Kyrgyz parliament adopted a resolution issuing a legally binding instruction to the prosecutor general's office, culture ministry and justice ministry to block access to the independent online news agency *Ferghana* (www.ferghananews.com) because of its coverage of last year's violence in the south of the country.

- Secret laws and decrees that govern security agencies, and provide permission to filter, block, or slow access to specific services and websites.

Pressure on service providers

- Monopolization or state control of Internet Service Providers and telecoms
- High tariffs for Internet access
- Pressuring ISPs for data access, mandating expensive filtering at the ISP level.

Extralegal responses

- Filtering, blocking, hacking, and pressure on intermediaries such as social networking sites
- DDoS, data-gathering for surveillance through traffic monitoring, spyware, and other unacknowledged tactics for disrupting access to or altering content.[13]

Propaganda, misinformation, disinformation campaigns, harassment

- Competing for influence in online forums, disinformation and misinformation on web 2.0 platforms, sometimes through paid networks of writers/bloggers or PR agencies
- Defamation, libel, false accusations to damage reputation[14]
- Harassment by security agencies to suppress speech.

Indirect methods

- Use of alternative governmental agencies to apply pressure, such as burdensome tax inspections, access to utilities, building code violations, and military conscription[15]
- Physical and psychological pressure, threats to self and family
- Violence, destruction of property, arson.

It is worth noting that the growth of mobile internet access has created another set of

[13] On March 30, 2011, the social networking site LiveJournal experienced a sustained DDoS attack. The target of the attack, in the opinion of many experts, appears to have been user Alexei Navalny, who is also the founder of the anti-corruption web platform Rospil. The attack rendered LiveJournal inaccessible on that day, and a second attacked achieved the same effect on April 4, 2011. Ashley Cleek: "Russia: DDoS Attack on LiveJournal Has Russians Debating Internet Politics," Global Voices Online, April 6, 2011, http://globalvoicesonline.org/2011/04/06/russia-ddos-attack-on-livejournal-has-russians-debating-internet-politics/.

[14] Authorities in Russia are harassing bloggers in the country, urging them to remove content and threatening them with judicial action. The Federal Security Service (FSB) asked the well-known blogger Leonid Kaganov, through his hosting company, to remove an anti-Semitic poem that he had mocked. Kaganov complied, but replaced the original poem with a parody. The FSB reiterated its request. Finally, for fear of further conflict with the security services, Kaganov decided to move his blog onto a foreign server. (source: Reporters Without Borders, personal communication, July 14, 2011). See also Alexey Sidorenko, Russia: Famous Sci-Fi Writer's Blog Removed for 'Anti-Semitism'," Global Voices Online, May 29, 2011, http://globalvoicesonline.org/2011/05/29/russia-famous-sci-fi-writers-blog-removed-for-anti-semitism/.

[15] In May 2011, an Azerbaijani district court sentenced the blogger Bakhtiyar Hajiyev, a Harvard graduate and former opposition candidate, to two years in prison on a charge of evading military service. He believes the trial is politically motivated and linked to his online activities. http://supportbakhtiyar.com/.

security, privacy, and information access and creation concerns. Mobile phones allow tracking, monitoring, and surveillance with relative ease. The fragmentary nature of privacy and anonymity controls with phones that allow tracking by location, by phone id number, by phone number, and SMS capture, make meaningful privacy a challenge in all states. Phone companies in the many countries have weak controls or ability to resist requests for data, either legally or extralegally.

Responses – what OSCE member states and the U.S. government can do

The documentation of these abuse tactics is reasonably well established, as reports referenced earlier in this document show, thanks to activist and freedom of expression watchdog activities. The OSCE should continue to support and promote monitoring and documentation of member states activities in this sector, both in their own work and in the work of civil society watchdog groups. A deeper question is the willingness of governments to apply political will to create positive incentives for citizens to participate in public spheres, pursuing both the letter and the spirit of commitments to OSCE rights obligations and Article 19 of the Universal Declaration of Human Rights. Those commitments are not just about the economic or scientific benefits of increasing Internet penetration, a concept that many FSU governments support, but about the political and civic rights of citizens. Without politically legitimate and accountable governance, the political will to foster those rights is unlikely to appear. To be clear – not every government in the former Soviet Union applies restrictions on online speech of the same measure or kind – the picture is varied across the region, with some countries working to meet their OSCE and UN obligations.

Unfortunately, the tendency of several OSCE member states from the former Soviet Union is in the direction of increasing control. A recent Commonwealth of Independent States framework law on Internet regulation, for instance, "contradict[s] the principles of online free expression and Net Neutrality by encouraging member states to exercise excessive control over what is a privileged space for exchanging information."[16] This document, intended as a guide for national parliaments in creating Internet regulation, seems to breech internationally accepted standards promoted by the OSCE in Net Neutrality and ISP data retention and access.

Responses to the failure of OSCE member states to abide by online freedom of speech principles begin with ideas behind the original Helsinki accords. Governments should be accountable to their own laws and their commitments under international agreements and treaties, and use legal, transparent, accountable regulations to manage internet access and content restrictions. Some basic principles for removing suppression of speech and discouraging self-censorship include:

- If filtering is necessary, place filter systems at the level of the user for maximum control; any filtering that goes on should be done in a transparent and accountable manner, so that citizens know who is responsible for it, how decisions about what

[16] Framework Law No. 36-9 "On the Bases of Internet Regulation,"
"Internet Regulation Should Not Curtail Freedom of Expression," Reporters Without Borders, June 15, 2011, http://en.rsf.org/europe-et-ex-urss-internet-regulation-should-not-15-06-2011,40463.html.

is or isn't filtered are made, there is a clear process for having such systems reversed, and that there are clear political consequences for officials who abuse the system, and regulatory consequences for companies that abuse it[17]

- Presume that the response to "bad" speech is more speech, and that restrictions on "bad" speech are proportionate and focused on specific incidents rather than classes of speech
- Ensure that restrictions and punishments are proportionate to the concern (for instance, domain-based filtering that also blocks legitimate content rather than the specific target is disproportionate)
- Apply laws consistently, without political or economic favor
- Avoid prior restraint measures such as indefinite enforcement of filtering
- Create clear legal terms for speech that is banned; there needs to be clear legal processes to appeal bans or for the overturning of bans. Banning must have a clear basis in the consent of the governed and must avoid the pitfall of reinforcing tyranny of the majority, and should be extremely rare
- Rely on independent courts rather than administrative bodies for enforcement
- Preferably, there will be no intermediary liability; if needed, clear rules of engagement, and response opportunities to requirements
- Encourage or even require corporate transparency with users and customers about what sorts of government surveillance and censorship demands are being made of them. The Google Transparency Report, which lists the number of government requests for hand-over of user information or deletion of content, is an excellent model[18]
- Do not filter the ISP level for IP issues; intermediary filtering of IP-related issues has negative speech freedom consequences.[19]

Beyond that, however, there are positive reinforcements that OSCE member states can follow, supporting both the letter and the spirit of their commitments to speech freedoms. From the perspective of citizen interests in online environments, this includes a focus not just on access to information, but on the opportunity for online participation, creation, and engagement. Online, in networked media environments, speech rights precipitate assembly, movement, and all other rights. Without the medium of speech, other rights are

[17] Some governments seek to justify filtering in response to hate speech, child pornography, and terrorism. Several studies suggest that filtering has a limited value in restricting this kind of speech, in particular child pornography. See: Cormac Callanan, Marco Gercke, Estelle De Marco, and Hein Dries-Ziekenheiner, *Internet blocking: balancing cybercrime responses in democratic societies* Aconite Internet Solutions, October 2009, online at: http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf "Child pornography: MEPs doubt effectiveness of blocking web access," European Parliament official website, November 15, 2010, at: http://www.europarl.europa.eu/en/pressroom/content/20101115IPR94729/html/Child-pornography-MEPs-doubt-effectiveness-of-blocking-web-access.

[18] http://www.google.com/transparencyreport/.

[19] "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation," Center for Democracy and Technology, April 2010, http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_(2010).pdf. Rashmi Rangnath, "Civil Society Walks Away from OECD Internet Policy Principles," Public Knowledge Blog, June 29, 2011, http://www.publicknowledge.org/blog/civil-society-groups-refuse-endorse-oecd-inte; "CSISAC Issues Statement on OECD Communique on Principles for Internet Policy-making," June 29, 2011, http://csisac.org/CSISAC_PR_06292011.pdf.

difficult to assert.

There has been in the past year an appearance of newly assertive civic voices in several OSCE countries that have poor records on government legitimacy issues such as free and fair elections, corruption, and repressive security regimes. The use of information technology tools and platforms that combine data analysis, visualization tools, mapping, community participation in reporting and mapping, and subject-specific expertise point to the creation of projects that are specifically designed to highlight corruption, create transparency, or demand governmental accountability. Examples include Help Map, which allowed Russian citizens to volunteer information and resources to fight fires in the summer of 2010, Roskomvzyatka, a crowdsourced map on which citizens can document instances of bribery, and Rospil, which crowdsources independent analyses of Russian government procurements. These projects show the potential that citizens in the former Soviet Union have to find creative solutions to their own problems. Such projects demonstrate that drivers of change often come from inside repressive environments, and that with greater connectivity, opportunities to participate can create meaningful change.

Supporting the continued openness and unfettered nature of the internet provides projects such as these with a firm foundations for the emergence of creative opportunities for people to express their citizenship. The OSCE role is best articulated as asserting that its members follow both the letter and the spirit of OSCE obligations.

The U.S. government role is best articulated as supporting the continued openness and unfettered nature of the internet. As a first step, the U.S. should consider how its policies on Internet freedom will effect local communities that they purport to help. It should follow a “do no harm” approach that is sensitive to local contexts and concerns, and takes into consideration the personal security and goals of online activists working in repressive contexts.[20]

In addition to voicing support for access, advocates should consider how to provide multi-faceted, diverse tools and resources that help people both to get access to information in restrictive environments, and perhaps more importantly, help people to create, share, preserve, and build the tools and resources that they need to be engaged citizens in their countries. Recent U.S. State Department initiatives to support a wide range of tools and education on information access creative content in countries that use extensive filtering and blocking is an example of the right kind of approach. Narrowly focusing resources only on information access to external information, on the other hand, downplays the importance of locally generated content, information technology tools, the opportunities for communities in repressive environments to strengthen their own content creation.

While building tools to help people participate freely online, protect identity and privacy, and participate freely in the exchange of information and knowledge is useful, it is ultimately not a substitute for the application of political will on the part of all OSCE member states to foster both legal environments and civic cultures of online participation,

[20] Ivan Sigal, “Going Local,” Index on Censorship, Vol 40, No. 1, 2011, p. 96.

to ensure that we protect and grow the Internet for citizens first, rather than security agencies or corporate interests. In this context, the U.S. has the opportunity to lead by example, whether in supporting open government data, as with the recent launch of the Open Government Partnership;[21] supporting Internet policy principles that represent the interests of citizens as well as corporations and governments, in forums such as the OECD; or ensuring that its cybersecurity policies do not impinge on the privacy and rights of its citizens, as with the ongoing debates over the extension of the Communications Assistance to Law Enforcement Act (CALEA) to facilitate surveillance.[22] [23]

Finally, governments interested in supporting these commitments should support information access, but also focus on creative capacity and removing barriers to civic participation. As a set of tools to respond to restrictive governments, removing both economic and political barriers to access is just the beginning. Governments interested in meeting the spirit of OSCE intent can offer many positive incentives to use and participation. These include:

- Internet infrastructure development
- Tariff pricing schemes that ease access costs in underdeveloped regions
- State programs to ensure internet access exists in schools, libraries, and other public contexts, and digital media literacy opportunities in those same facilities.
- Open government programs to systematically open government data to public scrutiny, allowing citizens to understand and track the workings of government.

[21] http://www.transparency-initiative.org/news/ogp-launch-july2011

[22] "CSISAC Issues Statement on OECD Communique on Principles for Internet Policy-making." See also Milton Mueller, "Civil Society Defects from OECD Policy Principles," Internet Governance Project, June 28, 2011, http://blog.internetgovernance.org/blog/_archives/2011/6/28/4847563.html. Full "Communique on Principles for Internet Policy-Making" available at http://www.oecd.org/dataoecd/40/21/48289796.pdf.

[23] Greg Nojeim, "Privacy and Security Are Not a Zero Sum Game," Center for Democracy & Technology, February 11, 2011, http://www.cdt.org/blogs/greg-nojeim/privacy-and-security-are-not-zero-sum-game.