COMMISSION ON SECURITY AND COOPERATION IN EUROPE

Opening Statement by Shelly Heald Han
Policy Advisor

Internet Freedom in the Age of Dictators and Terrorists
March 3, 2016

Good morning and welcome to the Commission on Security and Cooperation's briefing on Internet Freedom in the Age of dictators and terrorists. About a decade ago when the internet was spreading like wildfire around the world and more user-friendly networking apps were taking off, I, and a lot of other, people jumped on the internet freedom bandwagon and hailed the internet as a game changer for spreading democratic ideals to places that traditional media could not reach.

It was precisely because it was so powerful that the internet has moved into the crosshairs of governments—because, to put it in simplistic terms, the autocrats fear it because it might be used to usurp their power, and the democracies fear it because it might be used by criminals and terrorists. Congressman Chris Smith, Chairman of the Commission, introduced the Global Online Freedom Act in 2007 in recognition of this threat to online users, particularly in places like China. But since 2007, we've seen the China model of internet control spread throughout the world.

So while several years ago most of our fears about internet freedom centered on foreign governments, in the post-Snowden world the debate has shifted to include discussion of what the U.S. Government is doing to our online information. The Apple versus FBI case being the most recent example. Although it is often phrased as a privacy versus security issues, I think it is really a security versus security question, namely, the security of online user information and systems versus our overall security environment against terrorist threats. For me the question becomes: where do you draw the line? Should we strive to know every bit of communication that passes between potential terrorists? If so, at what cost?

In our discussion today, I do want to talk about U.S. law enforcement demands, but I also think it is just as important to remember that there are countries, like China and Russia, with the capability and the political means to do much worse. Here in the United States we have the mechanisms for substantive political debate, legislation, court cases, etc. Those options do not exist for the citizens of many, many other countries where the internet is both heavily censored and heavily monitored.

I'd like to turn now to our panelists now for their expert perspectives.

First is Rebecca MacKinnon, the Director of the Ranking Digital Rights Project which works to set global standards for how companies in the information and communications technology (ICT) sector and beyond should respect freedom of expression and privacy.

Author of *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books, 2012), Ms. MacKinnon is co-founder of the citizen media network Global Voices. She currently serves on the board of directors of the Committee to Protect Journalists and was a founding member of the Global Network Initiative.

Next is Lisl Brunner, responsible for GNI's policy development and learning program. Most recently, she was the Facilitator for the Telecommunications Industry Dialogue at GNI, where she coordinated a group of telecommunications operators and vendors addressing freedom of expression and privacy rights in the context of the UN Guiding Principles on Business and Human Rights.

And then Tim Maurer, associate at the Carnegie Endowment for International Peace. His work focuses on cyberspace and international affairs, with a concentration on global cybersecurity norms, human rights online, Internet governance, and their interlinkages. He is writing a book on cybersecurity and proxy actors.

Mr. Maurer serves as a member of the Research Advisory Network of the Global Commission on Internet Governance, the Freedom Online Coalition's cybersecurity working group "An Internet Free and Secure," and co-chaired the Civil Society Advisory Board of the Global Conference on CyberSpace.