



# HELSINKI COMMISSION BRIEFING

---

UNITED STATES COMMISSION ON  
SECURITY AND COOPERATION IN EUROPE

## Testimony :: Meg Roggensack

Senior Advisor, Business and Human Rights - Human Rights First

Chairman Smith, Co-Chairman Cardin, I wish to thank you and the Members of the Helsinki Commission for conducting this briefing and for your leadership efforts to promote respect for freedom of expression and privacy rights by information and communication technologies companies (ICTs).

Nearly two years ago, Secretary of State Hillary Clinton boldly declared “the freedom to connect” as a logical extension into cyberspace of the fundamental human rights of speech, expression, privacy and association. She warned of the consequences if we fail to protect this freedom:

[This issue] is about what kind of world we want and what kind of world we will inhabit. It’s about whether we live on a planet with one internet, one global community, and a common body of knowledge that benefits and unites us all, or a fragmented planet in which access to information and opportunity is dependent on where you live and the whims of censors.  
(emphasis ours)

Multinational companies operating in the Information and Communication Technology (ICT) sector are on the front lines in the emerging battle over whether we will realize the vision of “one internet” or succumb to pressures from repressive regimes and end up with a balkanized internet. They are on the receiving end of government demands to censor or limit service, to provide users’ personal information, or to facilitate surveillance. Their decisions have a wider impact on the ICT sector, and the level of openness and security all users enjoy.

The human rights challenges are significant, they evolve nearly as rapidly as ICT products and services themselves, and they affect a range of companies, from internet providers to telecommunications companies, credit card providers and manufacturers of mainframes and switching technology. In the past year alone, we’ve witnessed government takedowns of entire services, as well as specific content, in Egypt, Pakistan, Vietnam, Iran, Afghanistan, Libya, Indonesia, and India; Iran’s launch of a censored and controlled country-specific internet; China’s imposition of a warning system to chill Twitter users’ speech; and legislation in this country, such as the Senate’s Cybersecurity Act of 2012 (S.3414), that, while aimed at empowering companies to aid in the fight against cyber security threats, would give companies broad powers to engage in content monitoring and censorship, even where users have been

assured the company will not engage in such practices.

Recognizing the pivotal role that companies in the ICT and other internet-related sectors play, Secretary Clinton declared that “American companies need to make a principled stand. This needs to become part of our national brand.” A key part of that national brand, she noted, is the trust between companies and users—the trust that a company will promote the free flow of information online, protect users’ privacy, resist censorship, and ensure that the information that users communicate or receive through technology will not be used against them. Customers will choose to do business with the companies that they can trust to provide reliable and consistent service and to safeguard their personal information.

The UN Framework and Guiding Principles on Business and Human Rights provide an important global standard for both governments and companies. The Framework recognizes that States are principally responsible for protecting human rights – and for addressing abuses by private companies. But, acknowledging the governance gap that arises where governments either lack capacity to enforce laws or are themselves the perpetrators of human rights abuses, the Guiding Principles also recognize that companies have an obligation to respect human rights, and call on companies to exercise “due diligence” to ensure respect for human rights in their global operations. Both governments and companies have an additional responsibility to afford a remedy when human rights abuses occur.

Stated simply, due diligence means that a company must “know and show” – must identify the human rights risks and possible impacts of its global operations and develop appropriate policies and practices to address that risk, track progress, and publicly communicate that progress. These principles also apply to a company’s business partners. The pace of mergers and acquisitions in the ICT sector means that companies need to regularly reconsider their human rights risk exposure.

The Global Network Initiative is, at present, the only initiative that affords companies in the ICT sector a platform for addressing human rights due diligence in a comprehensive, credible and transparent way. The GNI’s multistakeholder structure brings together a range of experts and civil society networks to consider the challenges companies face and to bring the perspectives of users affected by government restrictions on freedom of expression and privacy online. Company members of the GNI pledge to adopt its Principles, based on international human rights norms, and to undergo independent assessments of their implementation of the Principles, including case examples. GNI’s implementation guidelines for their central principles call on companies to seek to clarify the scope and legal basis of government demands to censor content or breach user privacy, where possible to challenge such requests, to interpret government requests so as to minimize negative effects, and to communicate its policies to users, clearly and in a timely manner.

We helped to launch the GNI because we believe that voluntary multistakeholder initiatives can play a valuable role in helping companies to address the human rights risk of their global operations. Whether or not they succeed depends in major part on whether they can demonstrate a positive impact on the human rights at issue. The GNI’s effectiveness is only beginning to be established. We are still in the middle of our first assessment cycle. GNI’s

effectiveness in addressing threats to freedom of expression and privacy online will depend on the extent to which company assertions about what they have done to implement GNI's Principles can be verified through independent assessments, and transparent reporting on those assessments.

While GNI has made progress in expanding its membership, most companies in the ICT sector are not part of the conversation about protecting freedom of expression and privacy online. As a recent report from BSR notes, while ICT sector companies have significant impact on human rights, many companies in the ICT sector have limited human rights expertise outside the headquarters level, undervalue stakeholder engagement, and do at best limited reporting on their efforts to address human rights impacts. This suggests that we have a long way to go. As we have frequently noted, statements about company due diligence efforts cannot and should not be taken at face value – because there is no way to independently verify whether they have adequate policies in place, whether those policies are being effectively implemented, and how, if at all, the company is addressing government demands.

The Global Online Freedom Act has the potential to help ensure stronger US policy alignment and wider corporate engagement in this important conversation. The US government can and should do more to identify and respond to threats to internet freedom across all relevant agencies. The GOFA's reporting requirements will help to drive greater policy coordination and alignment. In addition, the GOFA zeroes in on the challenge of engaging the ICT sector more comprehensively, requiring that companies adopt due diligence policies. This requirement should help raise awareness within the sector and spark much needed debate about best practices. Human Rights First looks forward to working with you to develop the best possible bill.

The threats to internet freedom are pervasive and proliferating – as the headlines confirm. Without the full engagement of ICT companies in this battle, we can't realize the vision of "one internet." That vision is vitally important for the millions of people living under repressive regimes. The internet is their "virtual town square", as essential to them as to us, in preserving and promoting democracy and human rights in this century.