THE GLOBAL POLITICS OF INTERNET FREEDOM
A reflection on the 2012 Milton Wolf Seminar by Harriet Di Francesco

During the first session of the 2012 Milton Wolf Seminar, former Austrian ambassador and current director of the Diplomatic Academy of Vienna, Dr. Hans Winkler, asked the question, “Has the Westphalian notion of sovereignty disappeared?” He stressed that, when discussing information rights and national sovereignty, we must ask ourselves, “where does one right end and another begin?” These questions have a particular resonance for a student of international relations and law such as myself. For me, the debate over internet freedom and governance is a mere footnote in a perpetual battle of ideas about state sovereignty and the individual rights. During the Seminar, representatives of both state and society (government officials, journalists, and academics) put forward their assessments and offered solutions to several current quandaries: Does the internet represent a public space to all; and, if it does, to what extent can governments regulate that space? Can fundamental human rights, the right to free speech, expression, and assembly, be applied to the internet? And if so, how do they apply to this space?

Whilst the seminar participants did not reach a general consensus on these issues, most agreed that states continue to exert influence in cyber space. Participants pointed towards examples of state influence over the internet such as: Iranian and Chinese uses of internet filtering technologies, Western sponsorship of circumvention technologies designed to evade these filters, and the prosecution of organizations like Wikileaks by states like the United States, United Kingdom, and Sweden. My conclusion is that the Westphalian notion of sovereignty has not disappeared and, despite techno-utopian claims to the contrary, the rise of social media has not significantly undermined the role of the state in restricting or enhancing individual human rights of expression and assembly. Nowhere is this more evident than in the recent political crusade to protect and promote freedom on the Internet and the international implications of that this may have.

In January 2010 and December 2011, the US Secretary of State Hillary Clinton delivered high profile speeches on internet freedom, the first in Washington D.C. and the second at The Hague. On both occasions, Clinton endorsed a campaign to defend and advance the fundamental freedoms of everyone, everywhere, including online. She condemned various countries for assaulting this freedom and asserted the rights of individuals to express themselves and freely associate in all public spheres, saying,

the right to express one’s views, practice one’s faith, peacefully assemble with others to pursue political or social change – these are all rights to which all human beings are entitled, whether they choose to exercise them in a city square or an internet chat room.

For Clinton, current mechanisms of internet governance—that is, governance by a combination of government, private sector, and civil society actors—supports the free flow
of information and provides a means for freedom of expression. Countries that challenge this system not only violate human rights, but also create national barriers in cyberspace that undermine the global marketplace of ideas. One Seminar speaker reasserted that the current US policy is to foster this multi-stakeholder governance. “As a space,” she said, “[the internet] is analogous to the offline world, the same rules, laws, and principles apply.” According to the speaker, a “tool-based model” of the Internet, that is, a means through which governments can assert control, inevitably presupposes the suppression of individual freedom online. The fundamental problem with this argument is that the current multi-stakeholder internet governance approach does not always ensure the free flow of information, nor does it effectively ensure freedom of expression across borders. In fact, it often privileges states and corporations over individuals.

Current governance in many ways privileges internet corporations over individuals when it comes to their ability to shape how and what information flows across and within borders. Whilst social networking sites such as Facebook and Twitter provide avenues for individual expression, they also make more private information public. For the purposes of profit-maximization, corporations customize more and more of the Internet experience without the users’ consent. In other words, these corporations have disproportionate influence over the conditions through which end users seek and impart information over the Internet. Examples of this include: targeted advertising, a Facebook identity that “travels” with users even after they leave the site, and a Google search database that memorizes and organizes search histories. Furthermore, major social networking sites set their own guidelines and restrictions about what can and cannot be published online. They have the power to remove anything that is deemed objectionable, obscene, pornographic, or defamatory. On a basic level, the Internet is not a public space at all, but, increasingly, a patchwork of private and corporate interests that seek to profit from the management of users’ information.

Governments are thus able to outsource the process of internet regulation by lending the responsibility to these private web service providers. This practice was described by Robert Faris, Research Director of the Berkman Center for Internet and Society at Harvard University: “Because legal processes on an Internet scale are so difficult, if not impossible,” Faris said, “we see a retreat to the informal, that is, blocking and restriction.” Faris, whose recent research includes Internet content regulation, state censorship, and surveillance practices, argued that all countries recognize that there is no absolute freedom on the Internet and engage in some form of regulation. Because political processes are contingent upon a variety of social and cultural elements within countries, there are significant differences in sensitivities and standards across borders. Thus, it is extremely difficult to imagine a single, shared cyber space accepted by all communities and their governments.

Nowhere is the continuing relevance of Westphalian notions of internet sovereignty more clear than in the area of cybersecurity. The Cyber Intelligence Sharing and Protection Act (CISPA), currently under review in the US House of Representatives, proposes to codify government rights to information and surveillance of online activity as a means for tackling “cybercrime.” The proposed bill would make it easier for the US government and private companies to share information about cybersecurity threats. It does not, however, establish any limits on the type of information that can be shared or specify the appropriate uses of
that information. Rather, it clearly exonerates companies from any liability for handing over private information to government agencies. CISPA threatens to give the US government unprecedented powers to gather citizen information while overriding existing privacy legislation.

Privacy is another area that demonstrates the difference between the rhetoric and the reality of the US government position on internet freedom. Despite promoting individual rights online, the US State Department has engaged in extensive espionage on citizens and other political figures via the Internet. The most recent and well-known evidence of this are contained within the Wikileaks documents released in July 2009. Hillary Clinton herself ordered State Department employees to gather biometric information on the UN secretary general, Ban Ki-moon, and other leading diplomats. In 2010, another cable released via Wikileaks revealed that the State Department sought to protect Bush administration officials facing criminal investigation in Spain for permitting the torture of terrorist suspects. Rather than addressing this corruption on behalf of the world’s most powerful state actors, the US Department of Justice dealt with this by convening a grand jury in 2011 to investigate Julian Assange and Wikileaks’s role in leaking classified diplomatic and military documents. The State Department also pressured Visa, Paypal, and other major online payment companies to freeze all Wikileaks accounts and Amazon and other US-based ISPs to refuse to host Wikileaks sites. Furthermore, American Wikileaks activists have since been repeatedly harassed, detained at airports, and had their electronic possessions confiscated without the use of a warrant. What is striking about these examples is the fact that, despite fostering “multi-stakeholder governance” in favor of a “tool-based model,” the Internet continues to provide a means through which governments, even those that actively preach otherwise, can reassert their control and regulate social activity.

There doesn’t appear to be much hope for change, either. The Obama administration continues to prevent, as best it can, access to and discussion about the disclosed WikiLeaks documents. The State Department has warned students of international relations intending to apply for jobs in the federal government that posting WikiLeaks links on social media sites such as Facebook or Twitter would appear as a black mark on their security clearance checks. Federal employees are not allowed to access the documents and the Library of Congress, the largest in the world, has blocked access to them from their computers. It is naïve, therefore, to think that only specific countries (“authoritarian” ones) utilize the Internet to consolidate state power.

In recent years, censorship in some countries has expanded, at least in part, in reaction to the threat of American hegemony in the Internet, media, and cultural sphere. Since the 2011 Freedom Online Conference, governments such as Iran, China, Russia, and Turkey, have become more vocal in their fears that the United States is exploiting its dominance of cyberspace in order to promote its own political agenda. They have continued to bolster their domestic internet enterprises at the expense of foreign competitors. In 2009, Turkey launched an effort to create “the Anaposta,” a national filtered search engine that blocked over 20,000 sites. Iran followed in 2010 by banning Gmail and announcing its own national e-mail system. In the same year, Russia also announced plans to establish a national e-mail
and, in 2011, announced plans to develop a national search engine service. Thus, fresh attempts to prevent the fragmentation of a global cyberspace may in fact hasten the erection of barriers around national lines.

So what does the future hold for internet freedom? From a purely political perspective, any international effort to liberalize the Internet must be led by America, the biggest single force shaping the actions of other states. Clinton’s speech was highly ambitious and idealistic, but also dangerously hypocritical. This hubris has destroyed any credibility in American claims to protect individual rights online, especially from the point of view of potential rivals and other less-than-friendly governments to the US. The fact that other countries have sought to create national search engines to compete with privately-owned American companies like Google, Yahoo, and Microsoft, underscores the impotence of a US-led initiative to open up cyberspace. Personally, I think that it is unrealistic to expect that governments will scale back the regulation and control of the Internet on a global scale. Thus, the current US foreign policy will continue to face challenges that it itself has helped to create.

About the Author

Harriet Di Francesco
MA Student
School of Advanced International Studies in Bologna
Johns Hopkins University
Email: hdifran1[@]jhu.edu

Harriet Di Francesco was selected as an Emerging Scholar Delegate to the 2012 Milton Wolf Seminar. She is a Masters student at Johns Hopkins School of Advanced International Studies in Bologna. Studying International Relations, Harriet has chosen courses with a strong emphasis on economics and law. In a recent research paper, Harriet explored the paradox between traditional forms of international justice and the cosmopolitan idea that individuals are moral and legal subjects in a global civil society. She is fundamentally interested in the central notions and ideas behind theories of international politics and the ways in which these can be applied to the real world.
About the 2012 Milton Wolf Seminar
Launched in 2001, the Milton Wolf Seminar Series aims to deal with developing issues in diplomacy and journalism – both broadly defined. Using case studies such as Hungary, Iran, Syria, Egypt, and Tunisia, the 2012 Milton Wolf Seminar, Transitions Transformed: Ideas of Information and Democracy Post-2011 explored the evolving relationship between media and democratic transition in light of rapid technological change and the shifting structure and dynamics of the international communication system. The seminar was jointly organized by the Center for Global Communication Studies (CGCS) at the University of Pennsylvania’s Annenberg School for Communication, The American Austrian Foundation (AAF), and the Diplomatic Academy of Vienna (DA). More information about this and previous seminars is available on the Milton Wolf Seminar [website] [http://global.asc.upenn.edu] and our Facebook Page [https://www.facebook.com/MiltonWolfSeminar].